Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Evaluación de procedimientos de seguridad de la información utilizando ISO 27002 y COBIT. Caso de estudio: empresa de hidrocarburos

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTORES

Giuliana Jakeline GARCÍA PAREDES

Verónika Yaneth GUILLÉN CAMARENA

ASESOR

Jorge Santiago PANTOJA COLLANTES

Lima, Perú

2009

Referencia bibliográfica

García, G. & Guillén, V. (2009). *Evaluación de procedimientos de seguridad de la información utilizando ISO 27002 y COBIT. Caso de estudio: empresa de hidrocarburos*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Nuestro trabajo está dedicado:

A Dios, que nos dio la perseverancia necesaria para seguir con nuestros objetivos.

A nuestros padres, que con su ejemplo y apoyo han sido nuestro soporte durante las largas jornadas de trabajo.

AGRADECIMIENTOS

Agradecemos a:

Nuestros padres por todo el apoyo, comprensión y paciencia que han entregado sin pedir nada a cambio excepto nuestra superación profesional.

Nuestros familiares, compañeros de estudio y trabajo y amigos en general que de una u otra manera han hecho posible que nuestro estudio de investigación resulte en este documento.

RESUMEN

EVALUACIÓN DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO ISO27002 Y COBIT

Bach. García Paredes, Giuliana Jakeline
Bach. Guillén Camarena, Verónika Yaneth

Junio - 2009

Asesor	:	Jorge Pantoja Collantes
Grado	:	Tesis Pre-grado

La presente tesina pretende evaluar el nivel de madurez de los procedimientos de seguridad de la información de la empresa, mediante la aplicación de una metodología y propuesta de indicadores basados en un conjunto de buenas prácticas.
Para tal efecto, se plantea la aplicación de normas o buenas prácticas tales como ISO 27002 y COBIT, para platear una metodología de evaluación y la determinación del nivel de madurez en el que se encuentra. Se tomará como caso de estudio una organización real (PetroAmérica).

Palabras Claves:

Sistema de Gestión de la Seguridad de la Información (SGSI)
Normas ISO
COBIT
Estándares

Línea de investigación:

Gestión de TI

Sublínea de investigación:

Auditoria y Seguridad Informática.

ABSTRACT

EVALUATION OF THE INFORMATION SECURITY PROCESS USING ISO27002 AND COBIT

Bach. García Paredes, Giuliana Jakeline
Bach. Guillén Camarena, Verónika Yaneth

Junio - 2009

Adviser	:	Jorge Pantoja Collantes
Degree	:	Thesis of Pre-Degree

The present dissertation aims at evaluating the backup and restore process of the Information Security Management Systems developed in the organizations, through indicators that show their correct performance. For such effect, it is set up the use of ISO 27002 and COBIT, to make the necessary modifications in the process and measure the performance of it, determining also the maturity level where is. It will be taken as a case study a real organization (PetroAmérica).

Key words:

Information Security Management System (ISMS)
ISO Rules
COBIT
Standards

Research Line:

TI Management

Research Sub-Line:

Audit and Information Security

INTRODUCCIÓN

El presente trabajo de investigación busca evaluar el desempeño de los procedimientos de seguridad de la información en las empresas mediante el planteamiento de una metodología adecuada y determinar el nivel de madurez en el que se encuentran estos, siguiendo las normas de seguridad vigentes. Durante este proceso se plantearan nuevos indicadores y se propondrán cambios para la mejora del desempeño de la Seguridad de la Información. A partir de estos planteamientos, se pretende realizar una mejor gestión del área de Tecnología Informática (TI) y así, los resultados obtenidos podrán alinearse a los objetivos del negocio.

Actualmente muchas organizaciones consideran que la seguridad de la información es un punto vital a tomar en cuenta para prevenir las amenazas tanto externas como internas que impidan llevar de manera eficaz sus procesos, sin embargo, una vez establecidos los parámetros de seguridad no toman en cuenta los indicadores que este sistema les puede proporcionar, no solo para prevenir vulnerabilidades sino también para ser usados en la gestión y toma de decisiones que puedan incrementar sus oportunidades de negocio.

La empresa PetroAmérica[*1], tomada como caso de estudio, al ser una empresa transnacional cuenta con un Sistema de Gestión de Calidad aplicada al área de Dirección de Servicios de toda la corporación, la misma que contiene diversas políticas de seguridad pero que, al ser de carácter general, no se adecua de forma ideal a cada una de las filiales existentes, lo cual impide que se tengan las herramientas adecuadas para el correcto análisis y gestión de los procesos. Es por esto, que basándonos en los lineamientos dados por algunos marcos de trabajo y estándares de seguridad de la información, pretendemos analizar y evaluar procedimientos mediante indicadores que permitan obtener mejoras en la gestión de seguridad, y determinar el nivel de madurez en el que se encuentran así como realizar los cambios que se crean convenientes en los diversos procesos que involucren la Seguridad de la información.

[*1] *Por motivos de confidencialidad se realizó el cambio de nombre a la empresa.*

INDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

Capítulo 1: PLANTEAMIENTO DEL PROBLEMA

En este capítulo se define el problema que enfrenta las organizaciones en cuanto al tema de Seguridad de la Información, realizando una descripción de los antecedentes del referido problema. Se presenta, además, los objetivos, la justificación, alcances y limitaciones de la presente tesina. Asimismo, se plantea una propuesta de solución al problema

1.1 Antecedentes

En muchas organizaciones la seguridad de la información es tratada como un problema sólo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema organizativo y de gestión, lo que con lleva a que las organizaciones no sean capaces de afrontar ataques provenientes de todos los ángulos.

Actualmente, los usuarios de equipos informáticos consideran que tienen mayor conocimiento e información disponible acerca de temas de seguridad que en años anteriores; lo que les permite incrementar su nivel de confianza en relación a las medidas de seguridad a las que se refieren.

La escasa seguridad que hubo en los orígenes del Internet hizo saltar la alarma, de tal forma que la seguridad de la información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal. Del mismo modo, las grandes empresas saben que, el tener la certeza de que la información que poseen está debidamente resguardada, puede ser potencialmente efectivo para generarles ventajas competitivas.

Aún así, observamos que las organizaciones y las redes de información que poseen estas, sean de origen informático o no, afrontan cada vez más amenazas de seguridad: fraudes por computadora, sabotaje, espionaje, virus, delitos informáticos, robo de información interna, hackers, etc. Con el avance de la tecnología, estas amenazas se multiplican, crecen y se vuelven más sofisticadas de detener, día a día.

No es suficiente contar con tecnología sofisticada, la gestión implica conocer la situación de lo que queremos tratar y tener claro hacia donde queremos ir, es decir, determinar un objetivo y tomar las acciones necesarias para conseguirlo.

Por esta razón, la seguridad de la información tiene como objetivo proteger este activo, fundamental en una compañía, respecto a una amplia variedad de amenazas para finalmente minimizar los riesgos y poder asegurar resultados positivos en la relación costo/beneficio y en la rentabilidad.

De esta manera, para prevenir posibles daños y perjuicios, una organización necesita considerar todos los soportes básicos al momento de implementar una serie de controles, políticas y procedimientos destinados a preservar la seguridad de la información que esta maneja. Debido a esto, con el avance del tiempo, los sistemas de seguridad han ido evolucionando y han tomado como parámetros diversas normas creadas a su vez por instituciones de normalización reconocidas a nivel mundial.

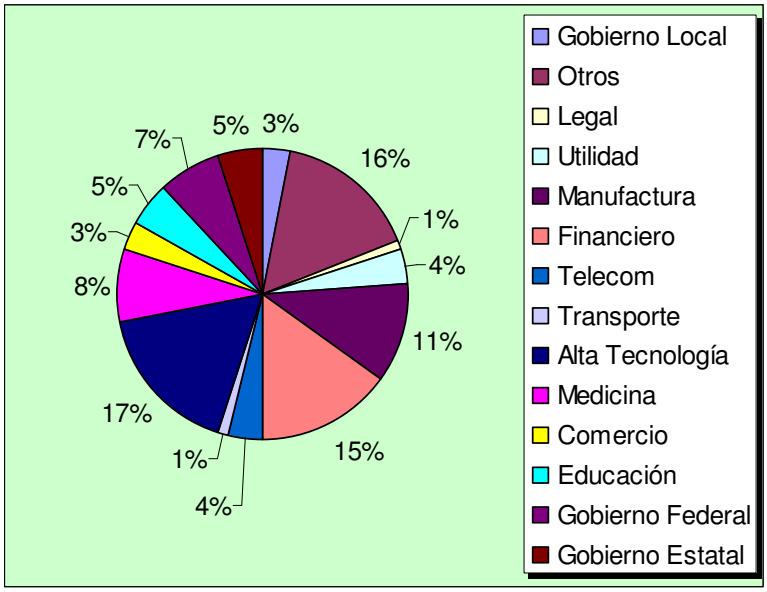
Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoria y fuera reconocido globalmente.

1.2 Situación de la Seguridad de Información

El uso de medios electrónicos de almacenamiento, proceso y transmisión de la información ha empeorado la seguridad de la información contra amenazas deliberadas de terceros. Debido a su valor intrínseco, desde siempre, la información ha estado amenazada de robo, alteración, destrucción, accesos no autorizados, etc. Muchas veces estas amenazas no solo provienen del exterior sino también del interior y pueden ser ocasionadas con o sin intencionalidad por parte de los mismos miembros de la organización.

A continuación vemos un cuadro en donde se aprecia la importancia que le dan las diversas industrias a la seguridad de la información (%), en este caso el 17% de las industrias relacionadas con la Alta Tecnología consideran que es importante mientras que solo el 1 % de el sector transporte encuestado considera que la seguridad de la información es importante.

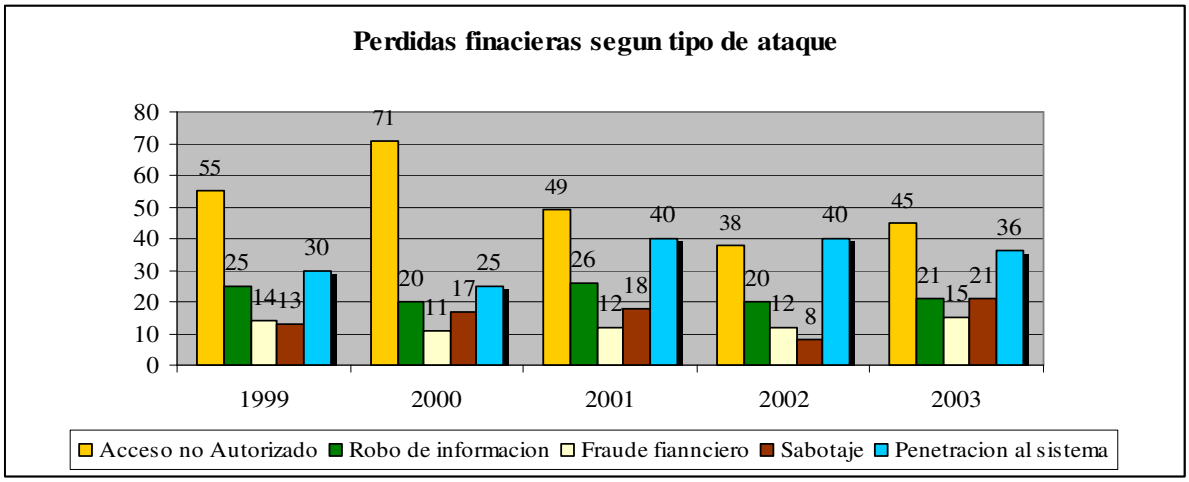
Figura 1. Encuestados según industria



Fuente: Ernest & Young

Esta falta de preocupación por mantener a salvo la información o por desconocimiento de su importancia se ve reflejada en perdidas financieras que se producían entre los años 1999 y 2003 aquí se puede apreciar que la mayor perdida financiera se ha dado en el tipo de ataque de accesos no autorizados siendo el año 2000 el de mayores

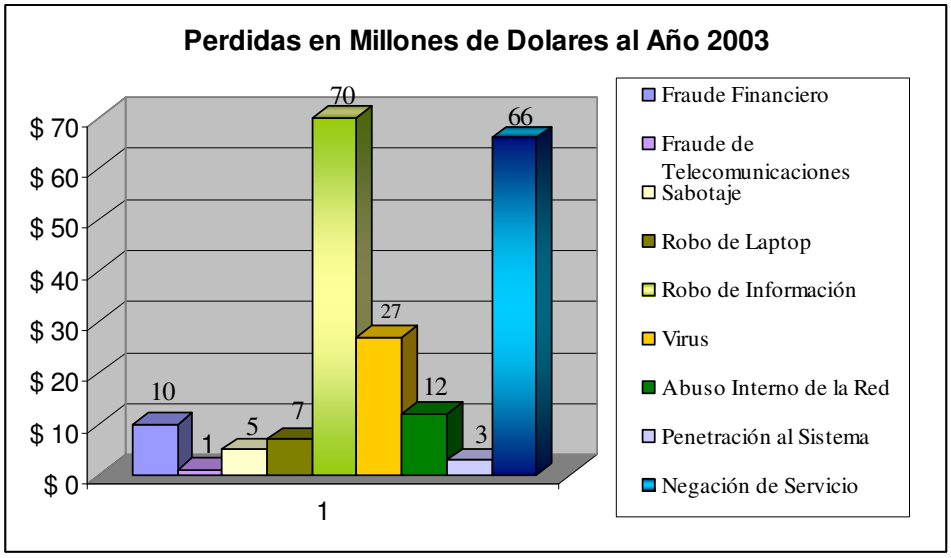
Figura 2. Perdidas financieras según tipo de ataque



Fuente: Ernest & Young

Para contrarrestar estas perdidas financieras algunas empresas emplearon algunas tecnologías de seguridad, entre las mas resaltantes que podemos ver en la grafica tenemos la seguridad física, firewalls, software antivirus y controles de acceso.

Figura 3. Perdidas en millones de dólares en el 2003



Fuente: Ernest & Young

La seguridad de la información se ha convertido en un asunto de alta prioridad dentro de las gerencias de las organizaciones de América Latina. Por medio de los siguientes gráficos obtenidos a través de encuestas podremos ver la respuesta de cada país, Argentina (Arg), Brasil (Bra), Chile (Chi), Colombia (Col), México (Mex), Venezuela (Vnz), ante las diferentes preguntas acerca de la Seguridad de la información, tales como ¿Cuán prioritaria es la seguridad de la información para la alta gerencia de su compañía? , ¿Cuánto confía usted en que su organización está protegida de amenazas internas a la seguridad de la información?, ¿su organización tiene instalados los requerimientos de seguridad necesarios para garantizar la continuidad del negocio a través de toda la organización?

Muchas organizaciones en Perú no definen adecuadamente las políticas que le permitan garantizar la continuidad del negocio a través de toda la organización, lo que s completamente distinto en otros países.

Aquí podemos notar como la mayoría de organizaciones garantizar la continuidad del negocio, a través de la implantación de estándares o normas de seguridad en al figura se aprecia que el 80% en Brasil garantiza dicha continuidad.

Figura 4. Su organización tiene instalados los requerimientos de seguridad necesarios para garantizar la continuidad del negocio a través de toda la organización

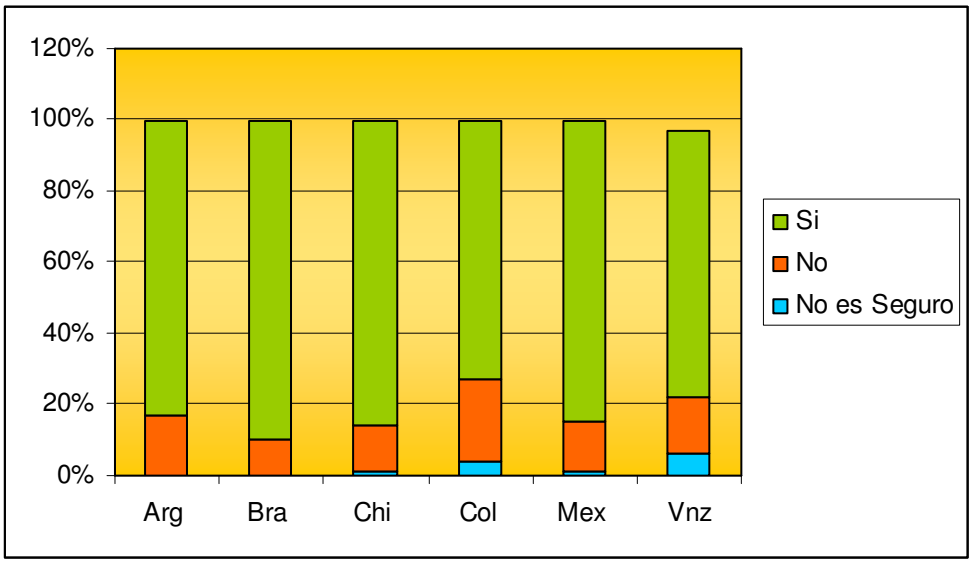


Tabla 1. Su organización tiene instalados los requerimientos de seguridad necesarios para garantizar la continuidad del negocio a través de toda la organización

		Arg	Bra	Chi	Col	Mex	Vnz
Si		83%	90%	86%	73%	85%	75%
No		17%	10%	13%	23%	14%	16%
No es Seguro		0%	0%	1%	4%	1%	6%

Fuente: Ernest & Young

Estas políticas implantadas para garantizar la continuidad del negocio necesitan ser conocidas por los empleados de la organización y para esto es necesario entrenar a los empleados.

Algunas empresas realizan este entrenamiento con mayor frecuencia, brindando capacitación a sus trabajadores al menos dos veces al año. Pero todo esto varia de acuerdo a la prioridad que la alta gerencia le de a la seguridad de la información, como se aprecia en la figura hasta el 2003 la mayor parte de las respuestas se orientan a la opción irregularmente o nunca.

Esto demuestra que solo cuando la Seguridad de la Información es una alta prioridad para la alta gerencia, esta se preocupa en actualizara sus empelados con las tendencias sobre este tema.

Figura 5. Con cuánta frecuencia su organización entrena a sus empleados acerca de políticas y procedimientos relacionados con la seguridad de la información

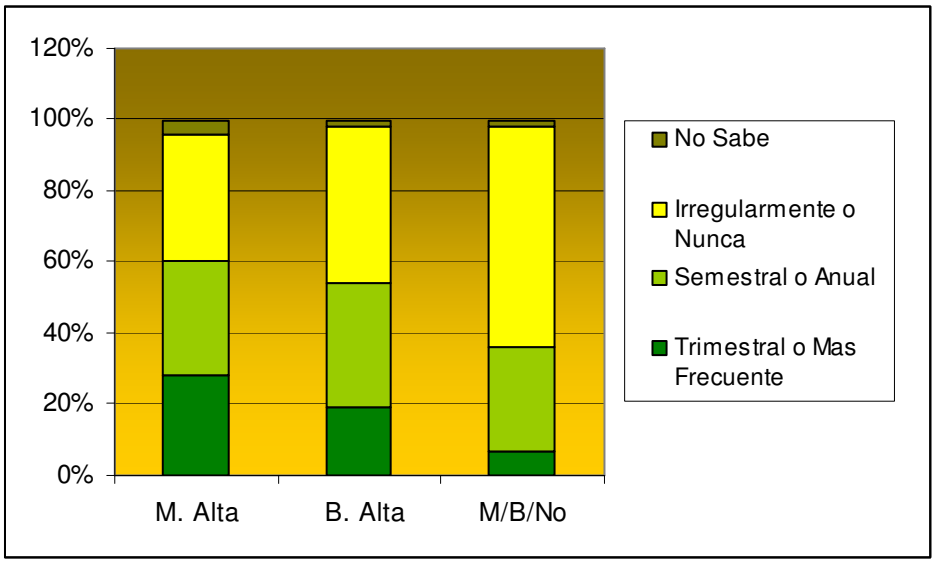


Tabla 2. Con cuánta frecuencia su organización entrena a sus empleados acerca de políticas y procedimientos relacionados con la seguridad de la información

		M. Alta	B. Alta	M/B/No
Trimestral o Mas Frecuente		28%	19%	7%
Semestral o Anual		32%	35%	29%
Irregularmente o Nunca		36%	44%	62%
No Sabe		4%	2%	2%

Fuente: CISCO

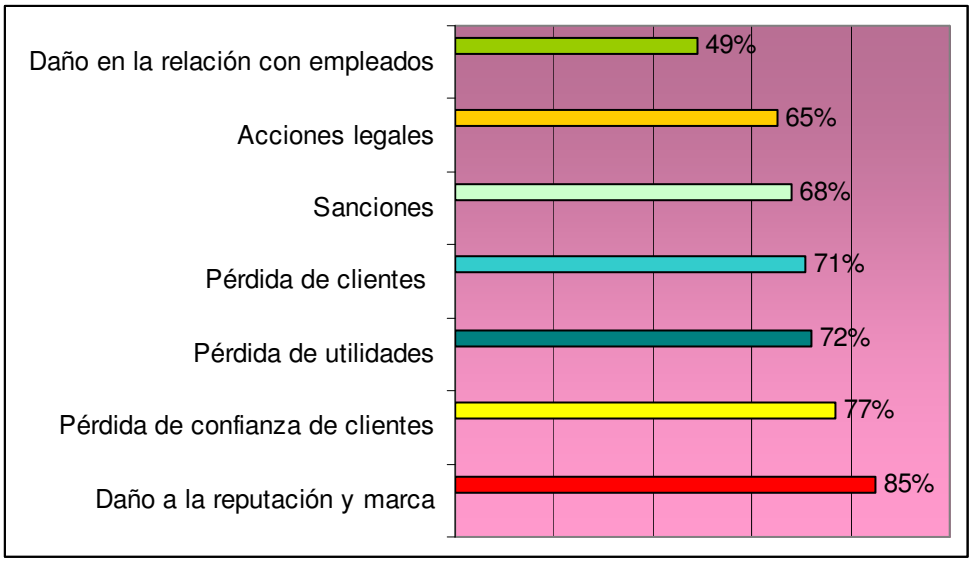
Esta falta de entrenamiento genera incidentes de seguridad de la información cuyas consecuencias podrían ser de gran impacto en la organización.

Estos porcentajes mostrados en la grafica están basados en respuestas dadas de "importantes" o "muy importantes".

Como podemos apreciar el daño en la reputación y marca de la empresa es considerado la más importante consecuencia de un incidente de seguridad de la información en es por eso que tiene un 85%. Este resultado en combinación con Pérdida de confianza de clientes, Pérdida de utilidades, Pérdida de clientes son indicadores claros de por que la seguridad de la información es parte importante en las organizaciones. El resultado de la encuesta refleja que la confianza de los clientes y el "nombre" en una empresa puede costar años en construirla pero puede ser severamente dañada en estos incidentes de seguridad,

demostrando lo costoso que puede ser un fallo en al seguridad de la información haciendo vulnerable a la empresa.

Figura 6. Cuales son las consecuencias de incidentes de seguridad de la información



Fuente: CISCO

Tabla 3. Cuales son las consecuencias de incidentes de seguridad de la información

Daño a la reputación y marca	85%
Pérdida de confianza de clientes	77%
Pérdida de utilidades	72%
Pérdida de clientes	71%
Sanciones	68%
Acciones legales	65%
Daño en la relación con empleados	49%

Fuente: CISCO

1.3 Definición del problema

El problema se centra en la necesidad que tiene la empresa de medir el buen desempeño y cumplimiento de sus normas de seguridad de la información, entre ellas las de resguardo y recuperación, y determinar el nivel de madurez en el que se encuentran, para proponer acciones y corregir errores.

Es importante mencionar que la empresa no posee un Sistema de seguridad de la información formal por lo que sus políticas o normas de seguridad se encuentran contenidas en un Sistema de Gestión de Calidad (SGC), haciendo difícil el manejo de estas normas por parte del área de TI.

Lo planteado líneas arriba imposibilita que se pueda asegurar la confidencialidad, integridad y disponibilidad del flujo de información existente que permite la continuidad de los procesos del negocio que le permitan mantener su competitividad en el mercado. Además origina en la empresa una serie de hechos los cuales se mencionan a continuación:

- Pérdida de información por errores en los sistemas de información o en la operativa de las personas
- El área de TI no atiende los requerimientos de cambio a los sistemas con la prontitud requerida.
- Accesos indebidos a información sensible de la organización.
- El conocimiento de las actividades del proceso esté en la mente de pocas personas.
- Ausencia de responsables por cada proceso en la empresa
- Vulnerabilidad en la información sensible de la empresa frente a ataques externos o internos.
- El proceso y sus actividades no cuentan con indicadores de desempeño.

1.4 Objetivos

1.4.1 Objetivo Principal

Establecer el nivel de madurez de los procedimientos de seguridad de la información aplicando una metodología y proponiendo indicadores tomando como base ISO 27002 y COBIT.

1.4.2 Objetivos Secundarios

- Definir y/o modificar una metodología aplicada a procedimientos de seguridad de la información.
- Analizar, rediseñar, implementar y probar el procedimiento de respaldo y restauración de la información mediante ISO 27002
- Definir el proceso de manejo de medios de almacenamiento mediante ISO 27002
- Definir indicadores para los procedimientos evaluados tomando referencia COBIT
- Servir de apoyo al CSO en la toma de decisiones tomando como base los resultados obtenidos en la evaluación de los procedimientos.

1.5 Justificación

Desde el punto de vista teórico, el presente trabajo de investigación permitirá conocer y entender las normas establecidas por ISO27002, así como los controles e indicadores establecidos en COBIT, los cuales nos permitirán establecer una metodología y evaluar en nivel de madurez de los procedimientos de SI.

Desde el punto de vista práctico, la presente investigación pretende analizar los procedimientos de seguridad de la información y evaluar su nivel de madurez, así como la creación, modificación y aplicación de las normas y políticas de seguridad de la empresa del caso de estudio utilizando la metodología propuesta, tomando como base los parámetros indicados en ISO27002 y COBIT los cuales nos permitirán también definir y/o modificar indicadores; todo esto dentro de un ciclo de mejora continua basada en el conocido “Ciclo de Deming” o PDCA (Plan, Do, Check, Act).

Desde el punto de vista metodológico, la investigación se basará en los requisitos y las mejores prácticas propuestas por las normas de la serie 27000:

- ISO 27002: Anteriormente denominada ISO17799: 2005. Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles. Será tomado como base para el establecimiento y modificación de políticas de seguridad.
- COBIT: Brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Se tomará como referencia los indicadores relacionados al logro de metas y desempeño y los niveles de madurez establecidos para determinar la situación de los procedimientos de seguridad de la información.

1.6 Alcances y Limitaciones

Debido a la gran amplitud de procedimientos o buenas prácticas relacionadas con los procedimientos de Seguridad de la Información, la presente investigación está orientada al estudio del proceso de Resguardo y Recuperación de Datos de Servidores, el cual está ya planteado en cierta escala pero que necesita ser analizado y reestructurado para un mejor desempeño, teniendo como premisa que aquellos controles que no pueden ser medibles no aportan nada a las metas que se esperan alcanzar, tal como se referencia en la Introducción de la norma ISO 27004 aún no publicada y que dice lo siguiente:

"El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras."[1]

Se implementará también el proceso de manejo de medios de almacenamiento puesto que en la actualidad no se cuenta con ningún procedimiento que realice la gestión de estos.

Basaremos el estudio del proceso tomando en cuenta lo considerado en la norma ISO/IEC 27002:2005, así como la definición o establecimiento de mejoras en los indicadores y niveles de madurez según lo establecido por COBIT.

1.7 Organización de la tesina

La presente tesina se compone de 7 capítulos. En el Capitulo 2, se presenta el marco teórico incluyendo definiciones de relevancia como Seguridad de la información, indicadores, ISO 2700 y COBIT entre otras. En el Capitulo 3, se presenta el Estado del Arte en el que se puede observar como otras organizaciones aplicaron las diferentes normas que se mencionan en capitulo anterior.. El Capitulo 4 muestra la metodología a seguir desarrollada a partir de los modelos presentados en el capítulo anterior, los cuáles nos servirán como base para la resolución del problema planteado.

El capítulo 5 presenta una descripción de la empresa que actuará como caso de estudio para el presente trabajo, así como de su organización y otros aspectos relevantes. En el capítulo 6, aplicaremos la metodología señalada en el capítulo 4 para el estudio y evaluación del proceso señalado y la creación de indicadores de acuerdo a las normas

[1] Tomado de www.iso27000.es

tomadas en consideración. En el capítulo 7 se realiza un análisis de los resultados obtenidos después de haber realizado los cambios en el proceso.

Finalmente en el capítulo 8, se presentarán las conclusiones y recomendaciones derivadas de la presente tesina.

Capítulo 2: MARCO TEÓRICO

En el presente capítulo se presenta el marco teórico que permitirá conocer los conceptos básicos para la comprensión del tema de investigación a ser tratado en la presente tesina.

2.1 Seguridad de la Información

La información de la empresa es uno de los activos más importantes que poseen y tiene un valor para la organización y por lo tanto se debería desarrollar mecanismos que aseguren una protección adecuada. Los objetivos de la seguridad de la información son proteger a la organización de amenazas, minimizar los años y maximizar el retorno de las inversiones y las oportunidades del negocio.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad:

Figura 7. Pilares de la información.

- Confidencialidad: Acceso a la información por parte únicamente de quienes están autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.
- Disponibilidad: acceso a la información y sus activos asociados por parte de los usuarios autorizados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto apropiado de controles, que pueden ser políticas, procedimientos, estructuras organizativas y funciones de software.

2.2 Sistema de Gestión de Seguridad de la Información (SGSI)

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Debe entenderse a la seguridad como algo integral. Debe abordar problemas desde tráfico en red, hasta seguridad física de servidores y bases de datos de información.

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.

Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Podría considerarse, por analogía con una norma tan conocida como la ISO 9000, como el sistema de calidad para la seguridad de la información.[2]

El cumplimiento de la legalidad, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

Garantizar un nivel de protección total es casi imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma

[2] www.iso27000.es

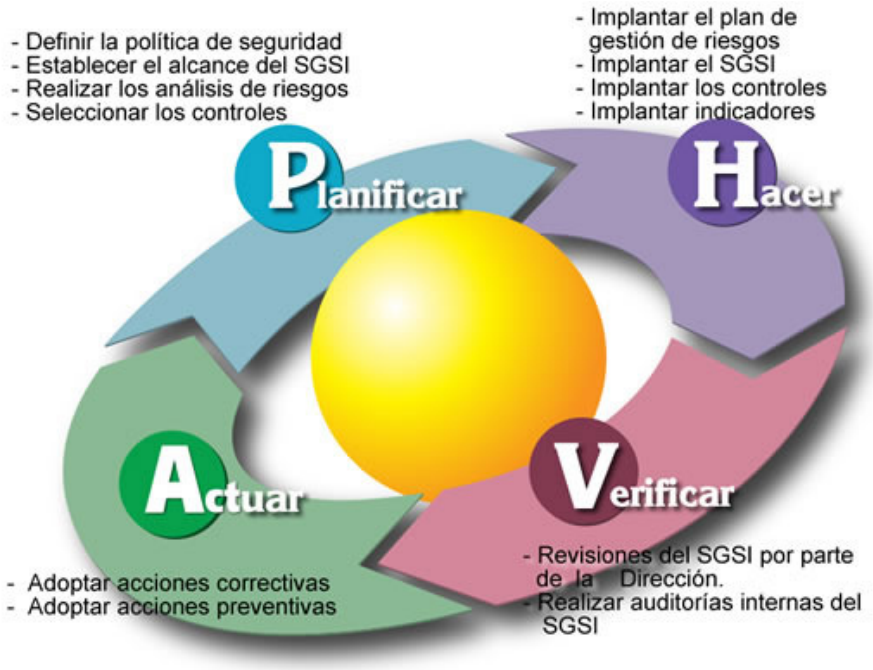
documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

2.3 Ciclo de Deming o PDCA

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27002, se utiliza el ciclo continuo PDCA; tradicional en los sistemas de gestión de la calidad.

A continuación se describen los pasos a seguir para la implementación del SGSI:

Figura 8. Ciclo PDCA para SGSI



Fuente: Iso 27000

2.3.1 Plan (Establecer el SGSI)

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

- Definir una política de seguridad.
- Definir una metodología de evaluación del riesgo.

- Identificar los riesgos.
- Analizar y evaluar los riesgos.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos.
- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya objetivos de control y controles seleccionados

2.3.2 Do (Implementar y Utilizar el SGSI)

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos
- Implementar los controles ya seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

2.3.3 Check (Monitorizar y revisar el SGSI)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para detectar a tiempo los errores, identificar brechas, etc.
- Revisar regularmente la efectividad del SGSI.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo.
- Realizar periódicamente auditorias internas del SGSI en intervalos planificados.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

2.3.4 Act (Mantener y mejorar el SGSI)

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de *Act* lleva de nuevo a la fase de *Plan* para iniciar un nuevo ciclo de las cuatro fases. Se debe tener en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

2.4 Métrica:

"La métrica es el método de medición definido y la escala de medición."[3]

"Métrica es una medida que proporciona una indicación cuantitativa de la extensión, cantidad, dimensiones, capacidad o tamaño de algunos atributos de un proceso o producto."[4]

Métrica es la correspondencia de un dominio empírico (mundo real) a un mundo formal, matemático. La *medida "i*ncluye al valor numérico o nominal asignado al *atributo* de un *ente* por medio de dicha correspondencia." [5]

La clave de las métricas de seguridad está en obtener medidas que tengan las siguientes características ideales:

- Deberían medir cosas significativas para la organización.
- Deberían ser reproducibles.
- Deberían ser objetivas e imparciales.
- Deberían ser capaces de medir algún tipo de progresión a lo largo del tiempo.

Cabe resaltar que las métricas no pueden interpretar por sí solas un concepto medible. Es por eso que se necesitan indicadores, ya que son el fundamento de los indicadores.

2.5 Indicadores

Un indicador es el método de cálculo que busca proveer una evaluación o estimación de un concepto medible con respecto a una necesidad de información.

Un indicador es una métrica o combinación de métricas que proporcionan una visión profunda del proceso.

Los indicadores revisten especial importancia en los estudios métricos. Cada estudio utiliza una serie de indicadores particulares. De su selección depende, en gran medida, la calidad y el impacto de la investigación final. Ellos proporcionan información cuantitativa y objetiva sobre los resultados del proceso de investigación, su volumen, evolución, visibilidad, estructura, etcétera.

[3] ISO 14598-1:1999
[4] Navarro, 2006
[5] Fenton, 2005

Los indicadores sirven para:

- Servir de base para cuantificar conceptos medibles para una necesidad de Información
- Servir de base a Métodos Cuantitativos de Evaluación o Predicción
- Los indicadores ofrecen información para la toma de decisiones

2.5.1 KGI (Key Goal Indicator o Indicadores Clave de Meta)

Es un indicador usado para decidir si las metas estratégicas de las compañías son logradas o no, y esto es usualmente presentado como un objetivo de valor. Se enfocan en el "que".

KGI es un indicador para tomar decisiones sobre el estado de los logros de los procesos del negocio que impactan el logro de los objetivos. KGI define criterios para el logro de objetivos.

Ejemplos:

- # y tipo de accesos sospechoso
- % de usuarios quienes no cumplen con los estándares de password
- # y tipo de código malicioso prevenido

2.5.2 KPI (Key Performance Indicador o Indicadores Clave de Desempeño)

Es un indicador que es usado para aprovechar el estado del proceso de negocio y el impacto de las metas estratégicas de las compañías. Se enfocan en el "como"

Es un indicador que nos dice si una compañía esta moviéndose en la dirección correcta hacia sus metas o no. Un indicador clave de meta es definido como una medida de "que" tiene que ser logrado a comparación de un Indicador Clave de Desempeño que es definido como una medida de "cuan bien" el proceso es interpretado.

Según algunos autores, un indicador clave de meta es definido como una medida de qué ha sido logrado a comparación de un indicador clave de desempeño que es definido como una medida de cuan bien el proceso se esta desempeñando. Está también indicado que su relación busca medidas de resultados de metas y medidas de desempeño relacionados a los habilitadores que harán posible que las metas sean logradas.

Ejemplos:

- # y tipo de incidentes de seguridad
- # de no autorizados direcciones de IP, puertos y tipos de trafico denegados

- % de claves criptográficas comprometidas y revocadas
- # de accesos autorizados, revocados, reseteados o cambiados

2.6 Análisis GAP

El análisis GAP examina las diferencias entre la gestión actual y la información presupuestada. Los resultados obtenidos representan el grado en el que una empresa ha cumplido sus objetivos.

El proceso de análisis GAP implica determinar, documentar y aprobar la discrepancia entre la diferencia existente entre los requerimientos de negocio y las habilidades actuales. Una vez entendida la expectativa general de gestión en la industria, es posible comparar esa expectativa con el nivel de gestión al cual funciona normalmente la compañía. Esta comparación es el análisis GAP. Dicho análisis puede ser gestionado en el nivel estratégico u operacional de una organización.

El análisis de brechas "constituye un método de consultoría de ciclo corto como parte de la planeación estratégica aplicada"[6] y de efecto duradero en el desarrollo organizacional de los consultantes.

Sigue a la fase de auditoria del desempeño para ejecutar el plan estratégico de la organización y su utilidad radica en la mejora de la capacidad de los clientes de obtener logros por si mismos, mediante la participación de su personal clave.

2.7 ISM3

2.7.1 Definición

El Modelo de Madurez de la Gestión de la Seguridad de la Información (ISMMM o ISM3, del inglés Information Security Management Maturity Model) es un Standard para la gestión de la Seguridad, nos ofrece un nuevo enfoque para especificar, implementar, operar y evaluar SGSI.

Es compatible con la implantación de ISO 27001, CobiT, ITIL e ISO 9001 y fue desarrollado por el equipo del Consorcio ISM3 liderado por el español Vicente Aceituno que tiene como finalidad su publicación como estándar internacional. Cabe resaltar que, se puede utilizar este estándar, distribuirlo libremente respetando su contenido y los derechos de autor.

[6] Goodstein, 1998

Además:

- Está diseñado para ser aplicable a cualquier organización independientemente de su tamaño.
- Puede usarse para mejorar los sistemas ISM de la organización, resaltando diferencias entre el nivel actual y el nivel deseado de madurez.
- Emplea un enfoque cuantitativo para evaluar la madurez del sistema ISM de una organización y su ambiente de control de seguridad de la información.

Se utilizan cuatro modelos conceptuales:

- El Modelo de Gestión de la Seguridad de Información: proporciona un marco para identificar los procesos principales en un sistema ISM y evaluar su madurez.
- El Modelo Organizativo: proporciona una visión basada en responsabilidades de una organización;
- El Modelo de Sistema de Información: proporciona una manera de describir los componentes principales de los sistemas de información;
- Modelo de Seguridad Contextual: permite a una organización preparar su propia definición de seguridad ajustada al ambiente y misión de la organización.

2.7.2 Niveles de madurez

Se puede utilizar ISM3 tanto para el diseño de un SGSI apropiado al ambiente y circunstancias particulares de una organización, o para evaluar la madurez de un SGSI existente. Sea cual fuese el modo de uso, la selección de los procesos de los SGSI es flexible, dado que cada nivel de madurez requiere cierto conjunto de procesos. Los 5 niveles pretenden describir sistemas ISM consistentes y prácticos, con distintos niveles de madurez y sofisticación.

2.7.3 Niveles de Gestión de Seguridad

- General: Documentación
  El proceso de documentación tiene la función de garantizar que el proceso esté definido, sea robusto y repetible mediante la definición de documentos de estándares de calidad y ayuda a mantener el sistema ISM actualizado mediante los requerimientos de expiración y revisión de documentos.

- Gestión Estratégica
  Los accionistas son los Clientes de la gestión estratégica. La gestión estratégica es responsable ante los accionistas para el uso de los recursos a través de los acuerdos establecidos.

- Gestión Táctica
  La Gestión Estratégica es el Cliente de la Gestión Táctica con respecto a los Procesos ISM3. La Gestión Táctica es responsable ante la Gestión Estratégica del desempeño del sistema ISM y del uso de recursos.

- Gestión Operativa
  La Gestión Operativa informa al Chief Information Officer y al Equipo de gestión Táctico de la Seguridad de la Información.

2.8 Normas ISO 27000

2.8.1 Antecedentes

En 1995, aparece por primera vez la norma BS 7799, con el objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.
Esta se compone de dos partes:

- BS 7799-1: Es una guía de buenas prácticas, para la que no se establece un esquema de certificación.
- BS 7799-2: Fue publicada en 1998 y establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Despues de muchos años de revisioes y modificaciones se realizó la publicacion de la ISO/IEC 17799 en el año 2000.
En el 2005, revisó y actualizó el ISO 17799; la cual fue renombrada como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

2.8.2 Dominios de ISO 27002

La ISO 27002 posee 11 dominios detalladoa continuación:

- Politica de Seguridad
- Aspectos Organizativos de la Seguridad de la Información
- Gestión de Activos
- Seguridad ligada a los Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso

- Adquisición, desarrolo y mantenimiento de los sistemas de Información
- Gestión de incidentes en la Seguridad de la Información
- Gestión de la continuidad del negocio
- Cumplimiento

Figura 9. Dominios ISO 27000

Fuente : ISO2700.ES

Para la revisión de dominios, objetivos de control y controles detallados revisar Anexo I del presente trabajo.

2.9 COBIT

2.9.1 Definición

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica.

COBIT define las actividades de TI en un modelo de 34 procesos genéricos agrupados en 4 dominios:

- **Planear y Organizar (PO):** Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio.
- **Adquirir e Implementar (AI):** Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes.

- **Entregar y Dar Soporte (DS):** Cubre la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.
- **Monitorear y Evaluar (ME):** Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

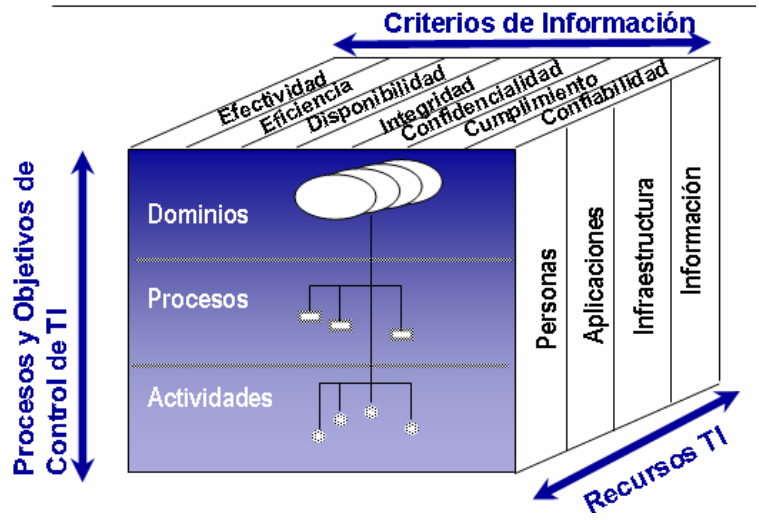
  Para la revisión de los procesos detallados de los cuatro dominios revisar Anexo II del presente trabajo.

2.9.2 Criterios de información y recursos de TI según COBIT

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- **Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- **Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- **Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada.
- **Integridad:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad:** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- **Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- **Confiabilidad:** de la información. Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Figura 10. Criterios de Información y recursos de TI



Fuente: IT Governance Institute

Los recursos de TI identificados en CobIT pueden identificarse/definirse como se muestra a continuación:

- **Datos:** Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- **Aplicaciones:** Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

- **Tecnología:** La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

- **Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información.

- **Personal:** Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

2.9.3 Modelo genérico de madurez

- **0 - No existente.** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

- **1 - Inicial.** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen

enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

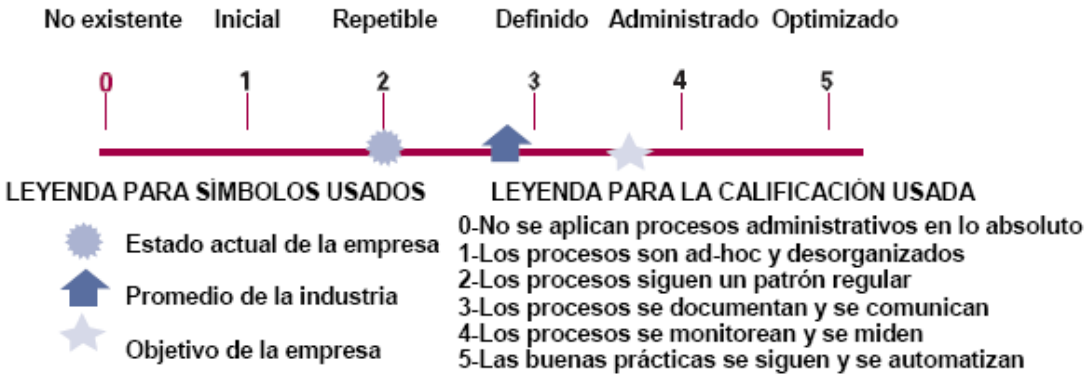
- **2 - Repetible.** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

- **3 - Definido**. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

- **4 - Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

- **5 - Optimizado.** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura 11. Representación gráfica de modelos de madurez



Fuente: IT Governance Institute

Capítulo 3: ESTADO DEL ARTE

En este capítulo revisaremos el estado actual de los objetivos de los marcos de referencia tocados en el capitulo anterior que estén enfocados al Proceso de Resguardo y Recuperación de Datos en Servidores.

Los marcos de referencia a utilizar son ISO 27002 y COBIT por lo que además, se mostrará el uso de estos en diversos casos de estudio que nos servirán de guía para la aplicación de la metodología creada.

3.1 ISO 27000

3.1.1 Gestión de respaldo y recuperación

Lo que se busca es mantener la integridad y la disponibilidad de los servicios relacionados con el manejo de información y comunicación, para esto se deberían establecer procedimientos de rutina que nos permitan conseguir la estrategia aceptada de respaldo haciendo copias de seguridad y realizando pruebas oportunas de recuperación.

- **Objetivo de Control: 10.5.1 Recuperación de la información**

El control sugiere hacer copias de seguridad de toda la información esencial del negocio y del software, en una frecuencia regular, en concordancia con la política establecida de recuperación.

Para esto debemos tener en cuenta ciertos puntos que son necesarios en la recuperación de información, tales como, almacenar un nivel mínimo de información de respaldo, conjuntamente con los registros de las copias de seguridad los cuales deben presentar exactitud y completitud así como procedimientos documentados de recuperación; las necesidades de la organización, los requisitos de seguridad de la información, y la criticidad de la información que permitan mantenerla continuidad de la organización deben verse plasmados en la frecuencia y extensión de los respaldos; la locación donde se almacenaran los respaldos deberá estar a una distancia prudente del local principal lo cual podrá mantener los respaldos a salvo ante cualquier desastre que pueda producirse y asimismo se le deberá dar a la información de respaldo una adecuada de protección física; se deberán realizar pruebas con una frecuencia regular a los medios de respaldo para comprobar su fiabilidad en caso de emergencia; los procedimientos de recuperación para asegurar su eficacia y su cumplimiento con los tiempos establecidos por los procedimientos operativos de recuperación deberán ser comprobados y probados

regularmente; se deberá proteger por medio de la encriptación los respaldos en casos en los que la confidencialidad sea importante.

En caso de los sistemas críticos, los arreglos auxiliares deben abarcar toda la información de los sistemas, sus aplicaciones y todos aquellos datos que sean necesarios de recuperarse del sistema completo en caso de un desastre. Estas copias de seguridad pueden automatizarse, lo cual sucede en algunas compañías.

3.1.2 Utilización de los medios de información

Se busca prevenir los accesos no autorizados, cambios, evitar daños a los activos e interrupciones de las actividades de la organización. Para esto los medios necesitan ser controlados y protegidos físicamente. Es necesario establecer procedimientos operativos adecuados que protejan los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de posibles. Se deberían documentar todos los procedimientos y niveles de autorización de acceso.

- **Objetivo de Control: 10.7.1 Gestión de medios removibles**

El control sugiere que deberían existir procedimientos específicos para la gestión de los medios informáticos removibles.

Para esto debemos tener en cuenta ciertas pautas que son necesarios para una adecuada gestión de los medios removibles tales como, eliminar la información contenida de todo medio reutilizable relacionada con la organización, cuando se considere que esta ya no es necesaria; todo medio desechado por la organización requiere un registro y autorización de tal eliminación lo cual permitirá guardar una pista de auditoria; los medios se deben almacenar en lugares que se consideren seguros de acuerdo con las especificaciones de los fabricantes; la información almacenada en el medio, que requiere estar disponible mayor tiempo que el tiempo de vida del medio debe ser también almacenada a fin de no perderla; la activación de medios removibles ser realizara solo cuando una razón de negocio.

- **Objetivo de Control: 10.7.2 Eliminación de medios**

El control sugiere eliminar los medios que no se necesiten utilizando procedimientos formales para que esto sea de manera segura.

Para poder lograr esto es necesario el establecimiento de procedimientos formales que minimizaran el riesgo de filtro de información sensible a personas externas para ello se

deberían considerar los siguientes puntos: la información sensible de la empresa deberá mantenerse a salvo a través de una adecuada eliminación del medio que la contenga (incineración, trituración o vaciado de datos de los medios); los procedimientos deben permitir identificar los puntos que puedan requerir un dispositivo de seguridad; realizar una adecuada selección de los proveedores que ofrecen servicios de recojo y eliminación de medios; es necesario realizar un registro de la eliminación de elementos sensibles para mantener una pista de auditoria.

3.1.3 Caso de Estudio:

A) Servicios S.A

Este caso de estudio se refiere a una empresa de servicios informáticos" Servicios S.A" que decidió implantar la ISO27002 para la Gestión de la Seguridad de la Información-, obteniendo como resultado importantes ventajas tanto para el área de TI como para el área de negocio.

"Servicios, S.A." es un proveedor de servicios informáticos así como hardware y software para clientes empresariales. Ellos solo contaban con una certificación en ISO 9002 obtenida hacía casi diez años, los empleados estaban acostumbrados a trabajar de forma mecánica y consecuente con directrices y procedimientos documentados. Sin embargo, el ambiente en la empresa había empeorado de un par de años hacia acá, no se tomaban en cuenta ciertos procesos relacionados con el resguardo, tales como la prueba de medios de almacenamiento, frecuencia en la realizaron de backups y se desconocía cual era la información critica de la empresa lo que impedía saber cuales backups contenían información sensible, ciertos procedimiento de resguardo no estaban documentados, existía una cantidad innecesaria de datos que no merecían la pena ser mantenidos. Al no cumplir con ciertos procedimientos no se encontraban preparados para afrontar una auditoria ya sea esta interna o externa. Debido a esto las decisiones de la dirección se tomaban más de forma instintiva, con poco análisis real. Con una rotación de personal en aumento, y la incapacidad para compartir conocimiento entre ellos, la dirección se dio cuenta de la necesidad de cambiar y analizó en profundidad las fortalezas y debilidades de la organización. La alta dirección de "Servicios, S.A." decidió implantar la ISO27002.

Ventajas directas

Incremento de la fiabilidad y seguridad de los sistemas: Como cualquier empresa, "Servicios, S.A." depende de los sistemas de información. La ISO27002 le garantiza tener controles que mantienen la disponibilidad de los sistemas y reducen el riesgo de que las vulnerabilidades sean explotadas, permitiendo también que el conocimiento que no era compartido por los empleados se vea plasmado en documentos y políticas a los cuales todos tengan acceso. Las auditorias internas de seguimiento y las externas de

recertificación aseguran que la empresa se mantiene al día en el conocimiento de las vulnerabilidades y buenas prácticas más recientes.

Incremento de beneficios: Las ventas y los márgenes se han incrementado y la percepción de la empresa por parte de los clientes ha mejorado. Se ha obtenido una certificación lo cual demuestra que se llegó a ser confiables y que ahora se puede asegurar los datos de los clientes, así como los propios de la empresa. Los clientes no sólo entienden que nuestra inversión en la ISO27002 les ha proporcionado beneficios a ellos, sino que están dispuestos a pagar un poco más por una infraestructura de IT segura. Ha habido un incremento en el beneficio final y es obvio que la mayoría de clientes prefiere tratar con empresas que tienen una certificación de seguridad reconocida. La implementación de la ISO27002 ha permitido el establecimiento de políticas que establecen los procedimientos adecuados para mantener un adecuado manejo de los medios así como el buen tratamiento de la información crítica de la organización.

Seguridad de la información rentable y coherente: Se implementó una seguridad eficiente de acuerdo a las necesidades de negocio, mejorando también el procedimiento de manejo de medios con información sensible y respaldando con una frecuencia establecida la información crítica para la continuidad de los procesos de negocio. La organización tenía muchas protecciones técnicas por toda la empresa, pero la mayoría de ellas al ser evaluadas proporcionaban poco o ningún beneficio empresarial y que por lo que al reconfigurarlas para proteger activos necesitados de un nivel de protección mayor proporcionaron un mejor retorno de la inversión. Todas las divisiones y departamentos habían desarrollado hasta el momento sus propias directrices de seguridad. La ISO27002 los ayudó a desarrollar un enfoque coherente de la seguridad a través de unas políticas uniformes basadas en las mejores prácticas de la industria.

Racionalización de sistemas: Se analizan adecuadamente los requerimientos de información y de seguridad lo cual significa ahora que se esta invirtiendo el dinero inteligentemente. Logrando recortar en cerca de un 50% nuestros sistemas y datos al darnos cuenta de que no merecía la pena mantenerlo.

C**onformidad con la legislación:** Al implantar la ISO27002 obligó a la empresa a cumplir con la legislación de su país Reino Unido en áreas como la protección de datos y el copyright de software.

Ventajas indirectas

Dentro de las ventajas indirectas podemos encontrar:

Mejora del control por parte de la dirección: La dirección tiene más control ahora sobre la organización y la información que maneja es de calidad para gestionar la misma; se

reduce, por tanto, el esfuerzo de la dirección en ese ámbito y se aprovecha para enfocarse en resolver otras necesidades de la organización y generar estrategias para ser competitivas en el mercado

Mejores relaciones interpersonales: el establecimiento de Políticas claras, procedimientos y directrices le facilitan las cosas a los trabajadores, mejorando el ambiente de trabajo y reduciendo la rotación de personal. La ISO27002 diferencia a "Servicios, S.A." de su competencia y le ha proporcionado un argumento de ventas único. La profesionalidad ha aumentado en toda la compañía. Dado que la seguridad depende en tan alto grado de los controles internos.

Mejor gestión del riesgo y planificación de contingencias: A través del proceso de certificación de ISO27002, "Servicios, S.A." identificó sus vulnerabilidades, amenazas e impactos potenciales en el negocio. Como resultado de esto e implementando controles de ISO27002, "Servicios, S.A." tiene un enfoque más estructurado de la gestión del riesgo. Por ejemplo, ahora se tiene un plan de continuidad de negocio que se ajusta a la empresa, no sólo al departamento de IT. En la evaluación de riesgos se identificaron los activos de información que son críticos para el éxito de la empresa. Permitiendo elaborar un plan de continuidad de negocio que priorizara dichos activos y reducir la exposición potencial a pérdidas financieras.

B) Caso Cambridgeshire Fire & Rescue Service

En abril de 2008, Cambridgeshire Fire & Rescue Service (CFRS) se convirtió en la primera seguradora en el Reino Unido que obtuvo la certificación ISO 27001 el estándar internacional del sistema de gestión de seguridad de la información (ISMS). Este caso de estudio destaca algunas de las etapas dominantes que CFRS cambio y considero criticas para lograr la certificación.

CFRS proporciona servicios a 700.000 personas en Cambridgeshire y a la ciudad de Peterborough.

Su proactividad es exactamente lo que ha adoptado CRFS para preservar la confidencialidad, la integridad y la disponibilidad de la información que maneja.
Como muchas otras empresas del mismo rubro, CFRS almacena y procesa información altamente confidencial y es dependiente en el análisis de sus datos, tales como manejo de estadísticas de incidentes, mejorar su funcionamiento operacional. Es por esto que las simples políticas implantadas no eran necesarias para cubrir todas las necesidades de la seguridad de la información viéndose en al necesidad de implementar ISO 27002.

Algo con lo que el Senior Management de CFRS estuvo de acuerdo era que el servicio no buscaba solución a corto plazo, rápida. Ellos querían una solución a largo plazo que estuviese basada en la mejora continua y lo que mejor encajaba en esto era ISO 27002 con su modelo de Deming (PDCA).
Se deseaba también un sistema de gerencia que involucre la organización que garantice también la seguridad por medio del establecimiento de controles y pruebas, así como permitirle hacer frente a los procesos de auditoria.
El estándar de la ISO 27002 permite establecer, operar, supervisar, repasar, mantener y mejorar el sistema de gerencia en ejecución.

Beneficios:

Ambiente mejorado de la seguridad

ISO 27002 ha proporcionado un gran marco de trabajo' alrededor de cuál la seguridad de la información puede ser construida. Ha conducido a una diferencia tangible en la cultura de organización. Hay, por ejemplo, un ambiente transparente en la divulgación de los de los incidentes de seguridad. Esto es absolutamente dominante para ser eficaces al poner acciones correctivas y preventivas.

Políticas más fuertes y procedimientos operacionales

Una de las actividades dominantes fue la desarrollar políticas mas fuertes así como identificar y documentar todos los procedimientos operacionales ligados ala seguridad de la información tales como manejo de medios, resguardo de datos, recuperación de datos, acceso entre otros. Es por eso que ha publicado ahora 23 nuevas políticas de seguridad.

La gerencia mayor es consciente que nunca se puede tener un ambiente el 100% seguro. Qué la certificación que ISO 27002 proporciona, sin embargo, es una forma de llevar a cabo de mejor modo el control de procedimientos a través de una mejora continua. Al implantar ISO27002 se ha logrado reducir el riesgo en al seguridad de la información.

3.2 COBIT

Para el presente trabajo y teniendo como enfoque el proceso de de Resguardo y Recuperación de Datos en Servidores, debemos centrarnos en el Dominio: Entregar y Dar Soporte, cuyo objetivo de control DS 11: Administración de Datos, se ajusta a nuestros objetivos.

3.2.1 DS11: Administración de Datos

Según lo establecido por COBIT, para administrar datos de manera efectiva se requiere de la identificación de requerimientos de datos. El administrar información es un proceso que además incluye el establecimiento de procedimientos que sean efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos nos ayudará a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

Tabla 4. Tabla resumen Objetivo DS 11

	Entregar y dar Soporte	Criterios de Información							Recursos de TI				
Dominio	**Proceso**	Efectividad	Eficiencia	Confidencialidad	**Integridad**	Disponibilidad	Cumplimiento	**Confiabilidad**	Recursos Humanos	Sistemas Información	Tecnología	Instalaciones	**Datos**
DS11	Administrar Datos				P			P					✓

Fuente: COBIT 4.0

Este objetivo de control trabaja sobre el proceso de TI de Administrar datos, y de esta manera, intenta satisfacer el requerimiento de negocio de TI del área a través de la optimización del uso de la información y la facultad de garantizar la disponibilidad de la información cuando se requiera enfocándose en mantener la integridad, exactitud, disponibilidad y protección de los datos.

Lo que se desea lograr a través del seguimiento de la norma es respaldar los datos y probar la restauración, administrar el almacenamiento de datos en el sitio y fuera del sitio, desechar de manera segura los datos y el equipo. Todo esto debe ser medido adecuadamente a través de la satisfacción del usuario con la disponibilidad de los datos, el porcentaje de restauraciones exitosas de datos, el número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados, entre otros indicadores requeridos.

Este objetivo de control tiene a su vez Objetivos más detallados, los cuales son:

- **DS11.1 Requerimientos del negocio para administración de datos**
  Busca plantear mecanismos para garantizar que el negocio reciba los documentos que espera, que sea procesasa toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

- **DS11.2 Acuerdos de almacenamiento y conservación**
  Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Se deben considerar en los procedimientos, los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad.

- **DS11.3 Sistema de administración de librerías de medios**
  Se deben definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

- **DS11.4 Eliminación**
  Prevenir el acceso a datos críticos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso mediante la definición e implementación de procedimientos. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse.

- **DS11.5 Respaldo y restauración**
  Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

- **DS11.6 Requerimientos de seguridad para la administración de datos**
  Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

3.2.2 Casos de Estudio

A) ADNOC, empresa de energía.

Adnoc es una compañía de energía integrada con 5,500 empleados con ganancias de más de $3 mil millones. Fundado en 1973, Adnoc comercializa y distribuye productos de petróleo y servicios dentro de los Emiratos Árabes Unidos e internacionalmente, es renombrada y respetada por su calidad excepcional y fiabilidad de sus productos y servicios.

¿Por qué escogió Adnoc implementar COBIT?

Adnoc estaba creciendo a pasos agigantados con el inicio de un proyecto de gas natural que aumentó la complejidad de su funcionamiento. No se aumentaron recursos proporcionalmente, no se priorizaron proyectos y el valor de TI fue cuestionado cada vez más. El mayor problema fue que no se estandarizaron muchos procesos de TI lo que contribuyó a la ineficacia en la entrega de servicios de TI.. Hay desafíos grandes que enfrenta TI tratando de satisfacer las expectativas del negocio.

Adnoc no había establecido procesos y procedimientos para proporcionar servicios de TI de una manera eficaz y eficaz. La compañía reconoció que las actividades eran dependientes en personas y no se documentó formalmente para que estas actividades puedan repetirse de una manera regular.. Esto también significó que no existieran mecanismos del mando para asegurar que las actividades se llevaran a cabo apropiadamente.

Además, TI no se alineó eficazmente al negocio para apoyar las metas de la organización. Por ejemplo, la priorización de las inversiones para varios proyectos de TI no se hicieron de una manera disciplinada. TI fue visto como un centro del costo, y la dirección no creyó que la inversión estaba justificada.

Los líderes de TI sugirieron implementar COBIT para añadir disciplina, mejorar el nivel de servicio, garantizar la confiabilidad de la información de los nuevos proyectos (el core del negocio), aumentar la satisfacción del usuario y mejorar las prácticas de gobierno de TI que permita al negocio lograr sus metas.

¿Por qué se pensó en COBIT como la mejor norma para usar?

Adnoc quiso abarcar todos sus procesos y vio que ninguna otra norma ofrecía el enfoque completo a todos los elementos de un proceso, incluso las métricas, los indicadores de desempeño (KPIs) y los indicadores de metas (KGIs). COBIT fue el más general y orientado al negocio que otras normas, además de abarcar la mayoría de los elementos del ambiente de TI que se posee, mientras otras normas se enfocan en un área indicada.

"Por ejemplo, ISO 27001 se direccional a los elementos de seguridad de información, mientras que COBIT va más allá de esto hacia una vista más panorámica de los procesos de una manera normal," dijo Ali Guidoum, Ph.D., CISM, supervisor de TI para ADNOC. "Sin embargo, no evita la aplicación de otras normas complementarias, de hecho, muchas otras normas se alinean con COBIT."

¿Cómo consiguió ADNOC que la Administración "comprara" COBIT?

El área de TI tuvo éxito explicando acerca del gobierno de TI y cómo COBIT ayudarían en la alineación de metas del área con las del negocio. TI también explicó a la dirección que si los

procesos que usan COBIT se regularizan, podría entregar los servicios más eficazmente en línea con las expectativas del negocio.

La presentación de casos de estudio del caso que ofrecen otras compañías exitosas donde COBIT también fue llevado a cabo dio la confianza a la dirección que COBIT es un modelo eficaz y útil para mejorar el gobierno y prácticas de TI existentes.

¿Cómo está usándose COBIT?

"La aplicación de COBIT en ADNOC fue encabezada por Bhavani Suresh que llevó a un equipo de casi 35 personas que contribuyeron al proyecto. Como resultado de los esfuerzos del equipo, todos los departamentos de TI: Operaciones de Centro de Datos, Automatización del Menudeo, Redes y Help Desk, y Sistemas de Aplicaciones están usando COBIT ahora."

Las secciones identificaron muchos procesos de COBIT que ellos juzgaron requisito para la aplicación. Sin embargo, para reducirlos a un número manejable, ADNOC usó COBIT para alinear sus metas comerciales a las metas de TI y entonces priorizó los procesos relacionados a través de una evaluación de riesgos.

ADNOC llevó a cabo los tres procesos más importantes y pertinente de COBIT, según el presupuesto de la organización y disponibilidad de los recursos. Los tres procesos seleccionados se enfocaron en la administración del cambio, administración de datos y administración del nivel de servicio.

Todas las secciones usaron un proceso de administración del cambio que se diseñó basado en COBIT para asegurar que se aplique de una manera controlada y minimizando las interrupciones a los servicios. El proceso de administración del cambio también ayuda a las áreas a seguir una norma, proceso sistemático que es repetible, medible y mejorado continuamente.

Adicionalmente, la administración del nivel de servicio (SLM) fue implementada en la organización entera. ADNOC adoptó un proceso SLM de COBIT que formalizó los acuerdos de niveles de servicio con otras unidades de negocios. El proceso SLM es continuamente mejorado basándose en el feedback de los ejecutivos comerciales.

El planeamiento de la continuidad del negocio fue otro proyecto significativo comenzado bajo COBIT. El marco de trabajo fue desarrollado, el modelo de continuidad comercial (BCM) se creó con roles claros y responsables, y se desarrollaron diferentes tipos de procedimientos. El BCM no fue específicamente un proyecto de TI ya que involucró diferentes áreas de la compañía, como Bienestar y seguridad, Recursos humanos, etc., y COBIT proporcionó el idioma común.

Otros procesos, como Administración de las configuraciones y Administración de la seguridad, también fueron diseñados y desarrollados basándose en COBIT.

Actualmente, ADNOC usa COBIT en combinación con otras prácticas, como las normas ITIL, ISO 27001 y PMBOK. Adicionalmente, los procesa de COBIT, incluyendo a la administración de datos, se ha identificado para la próxima fase de aplicación.

¿Qué beneficios obtuvo ADNOC usando COBIT?

La meta principal de la aplicación de COBIT era mejorar la eficiencia de la entrega de los servicios de sistemas de información mejorando los procesos existentes o diseñando e implementando nuevos procesos - y esta meta ha sido cumplida.

Aunque ADNOC era consciente que no todos los procesos de COBIT eran aplicables o requeridos, el ejercicio de priorizar ayudó a la compañía a hacer moldeable la aplicación y llevarla a cabo en fases. Los procesos lograron los resultados esperados y una mejora significante se notó en la eficacia de la entrega de servicios de TI. Ellos han llevado a la organización a la madurez y han sido incluidos en la cultura de TI.

Notando el éxito que alcanzó la primera fase de aplicación de COBIT, la compañía persigue ahora avanzar para contemplar más procesos de COBIT adicionales. Además, ADNOC está trabajando en la posibilidad de integrar COBIT con otras unidades de negocio para maximizar el beneficio. Se espera que tome uno a dos años lograr la integración sin costo entre las diferentes áreas.

B) Dongbu HiTek usa COBIT para incrementar los Niveles de Madurez

El número de empresas en Corea que usa COBIT como una herramienta de administración de TI ha aumentado drásticamente, según un reciente estudio. El estudio fue dirigido por el Prof. Lee Jung-Boon, vicepresidente del Capitulo ISACA de Corea.

Los resultados del estudio (Septiembre / Octubre 2008) indican que 44 de 97 empresas inspeccionadas habían adoptado COBIT— tres veces el número de usuarios de COBIT identificado en el estudio del último año. El estudio de este año también encontró que el porcentaje de empresas que adoptan su propia metodología ha disminuido de 64 a 46.

Una de estas compañías es Dongbu HiTek, un proveedor de la solución para dispositivos. Tiene su sede principal en Seul, Corea, con subsidiarias en el EE.UU., China y Taiwán. Dongbu HiTek ha estado en negocio por 12 años y actualmente tiene 2,500 empleados.

¿Por qué COBIT?

La compañía quiso regularizar sus procesos comerciales basados en estándares globales, complementándolo con K-SOX e ISO 27001, e implementó la administración de TI a través de RTE: Real Time Enterprise.

Dongbu HiTek decidió implementar COBIT porque contiene las mejores prácticas globales para los procesos de negocio de TI; es complementario con las mayores y más difundidas normas internacionales, incluso ÚTIL ya la serie ISO 27000, PMBOK, etc.; y proporciona un idioma común. La compañía usó Seis Sigma para ayudar con la implementación de COBIT.

Para ayudar a la compañía a implementar COBIT eficazmente, el Prof. Hwang K.T., presidente del Capitulo ISACA de Corea, presentó seminarios de COBIT y casos sugeridos. Basado en su guía, las metas principales de Dongbu HiTek para COBIT eran mejorar los procesos de TI y su performance. Esas metas se han logrado, con la organización que alcanza un nivel de madurez 4 para los procesos de Sarbanes-Oxley.

¿Cómo COBIT benefició Dongbu HiTek?

Además de levantar el nivel de madurez de la compañía para los procesos de Sarbanes-Oxley, COBIT ha ayudado a Dongbu HiTek a determina indicadores de meta e indicadores de performance importantes, y establecer responsabilidades claras a través de los mapas RACI.

Como resultado de la implementación exitosa y eficaz de COBIT en la compañía, Dongbu HiTek recibió, recientemente, el premio COBIT, patrocinado por el Capitulo ISACA de Corea.

¿Cuáles son los planes del futuro de Dongbu HiTek para COBIT?

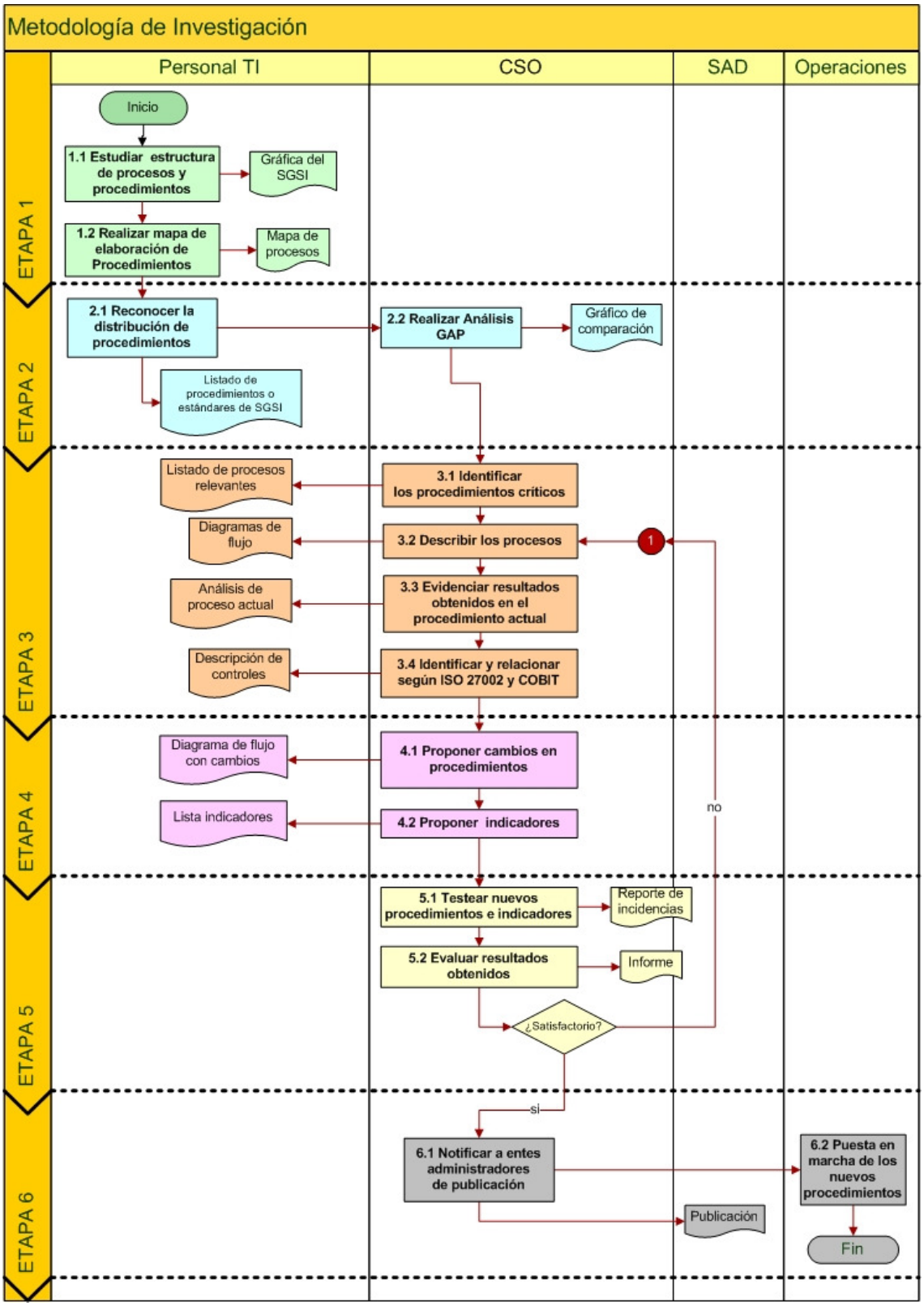
Dongbu HiTek planea continuar mejorando los procesos de TI a través de mejoras de la performance (meta de actividad => meta del proceso => meta de TI) e identificar y proponer iniciativas de cambio continuamente para mejorar los niveles de madurez.

Capítulo 4: METODOLOGÍA DE INVESTIGACIÓN

En este capitulo se explicara la metodología a usar para el desarrollo de la presente tesina. Para el tema que se está tratando se desarrollará la investigación aplicada tomando como base el modelo PDCA, tratando y explicado en el Capitulo 2, pero con unas ciertas modificaciones propuestas que servirán para un mejor análisis de los procedimientos a los cuáles nos enfocaremos.

Esta metodología esta orientada a empresas que ya tienen un sistema de gestión formado, aplicado y con cierto nivel de madurez pero que necesitan de una evaluación, análisis y reestructuración de ciertos procesos y procedimientos referidos a la Seguridad de la Información.

Figura 12. Detalle de la Metodología a Desarrollar

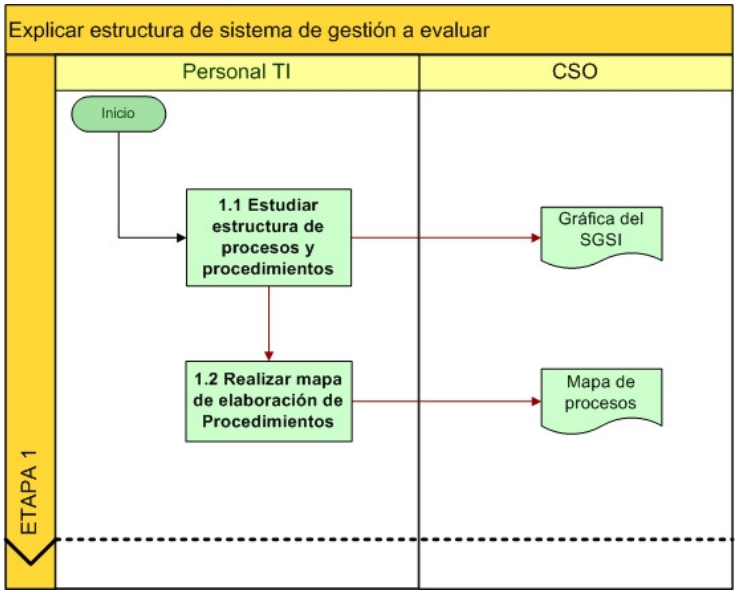


Fuente: Elaboración propia

4.1 1ra. Etapa: Explicar estructura de sistema de gestión a evaluar

En esta etapa se estudiará la estructura del sistema de gestión que actualmente emplea la empresa para obtener como resultado la importancia que esta le da a los requerimientos necesarios para asegurar la correcta gestión de los diversos procesos que maneja y de esta manera, sustentar la relevancia de las necesidades de mejora que afronta la empresa.

Figura 13. Metodología: Etapa 1



Fuente: Elaboración propia

4.1.1 Estudiar estructura de procesos y procedimientos:

- El **objetivo** es reconocer la forma de organización de los procesos y los procedimientos actuales de la organización mediante el estudio y entendimiento de la estructura de los sistemas de gestión existentes (de ser el caso).
- El **resultado** de esta tarea será una descripción breve y/o gráfica de la situación de la empresa antes, durante y después de realizado el trabajo planteado en la presente tesina.

4.1.2 Realizar mapa de elaboración de Procedimientos:

- El **objetivo** de la tarea es conocer la forma de realizar cambios a los procedimientos ya establecidos de tala manera que se sigan los lineamientos de la organización y así adaptarse a su forma de trabajo.

- El **resultado** será la presentación del mapa de procesos para la elaboración y/o modificación e procedimientos a los que nos deberemos ceñir para proponer los cambios en métricas e indicadores.

4.1.3 Cuadro resumen de la etapa

Tabla 5: Etapa 1: Objetivos y Resultados - Metodología de Investigación

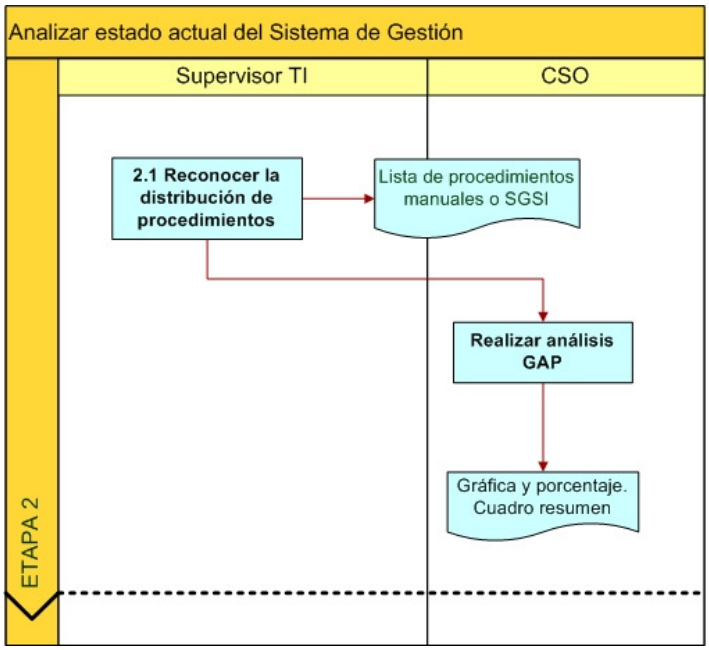
OBJETIVO	RESULTADO
Reconocer la organización de procesos y procedimientos.	Gráfico de la organización del sistema de gestión a evaluar.
Conocer el proceso para realizar modificaciones en procedimientos y procesos.	Mapa de procesos de la empresa a evaluar.

Fuente: Elaboración Propia

4.2 2da. Etapa: Analizar estado actual del Sistema de Gestión

Esta etapa tiene como fin reconocer, dentro del universo existente de documentación de la empresa en estudio cuales son los procedimientos y/o estándares enfocados a la Seguridad de la Información mediante un estudio en el cual se establezca el tipo de proceso y el macroproceso en donde están contenidos.

Figura 14. Metodología: Etapa 2



Fuente: Elaboración propia

4.2.1 Reconocer la distribución de procedimientos

- El **objetivo** de la tarea es reconocer que procedimientos serán considerados dentro de la tercera etapa del estudio mediante la identificación de la ubicación dentro del sistema de documentación que la empresa posea y el macroprocreso en donde esta contenido.
- El **resultado** será un listado de procedimientos, manuales o estándares referidos a la Seguridad de la Información identificados dentro del mapa de procesos existente para determinar el grado de interrelación existente con los procedimientos restantes.

4.2.2 Realizar Análisis GAP

- El **objetivo** de la tarea es identificar la cantidad de controles que proponen la normas ISO 27002 y que pueden ser soportados de una manera total o parcial por la situación actual de seguridad.
- El **resultado** será un gràfico de porcentaje, tabla resumen y un gráfico comparativo entre la cantidad de controles definidos y la cantidad de controles que son soportados actualmente por el modelo de gestión a evaluar.

4.2.3 Cuadro resumen de la etapa

Tabla 6: Etapa 2: Objetivos y Resultados - Metodología de Investigación

OBJETIVO	RESULTADO
Reconocimiento de procedimientos referentes a seguridad de la información	Listado de procedimientos, manuales o estándares establecidos
Identificar la cantidad de controles que proponen las normas ISO 27002 y que pueden ser soportados.	Gráfico de porcentaje de análisis GAP Cuadro Resumen de controles soportados Grafico comparativo de controles

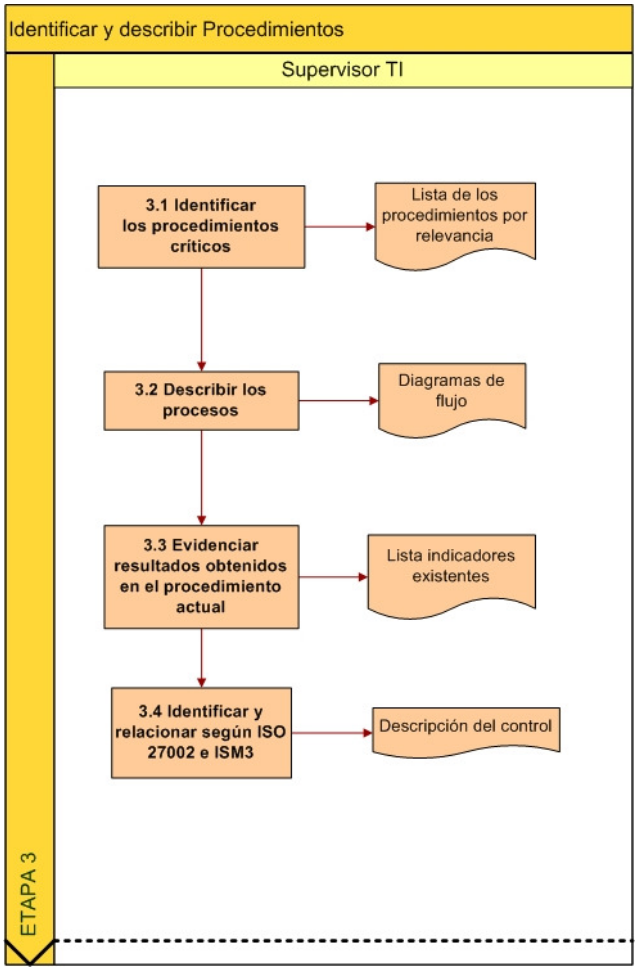
Fuente: Elaboración Propia

4.3 3ra. Etapa: Identificar y describir Procedimientos

Una vez concluido el análisis del estado de los procedimientos relacionados a la Seguridad de la Información procederemos a filtrar por orden de importancia aquellos que involucren procesos que son considerados críticos para el negocio.

De esta manera, se tratará en primera instancia los procedimientos enfocados a la seguridad que son desarrollados de manera continua y que son objeto de análisis diario.

Figura 15. Metodología: Etapa 3



Fuente: Elaboración propia

4.3.1 Identificar los procedimientos críticos

- El **objetivo** de la tarea es conocer la relevancia de los procedimientos, el cual debe ser obtenido a partir de una ponderación la cual tome en cuenta las caracterìsticas principales de dichos procedimientos.
- El **resultado** será un cuadro de los procedimientos y su relevancia en el sistema de gestión de seguridad de la empresa.

4.3.2 Describir los procesos

- El **objetivo** de la tarea es entender de manera gráfica la relación que se da entre los procesos , los actores y los documentos obtenidos en un procedimiento ya establecidos
- El **resultado** serán los diagramas de flujo corespondientes al proceso.

4.3.3 Evidenciar resultados obtenidos en el procedimiento actual

- El **objetivo** de la tarea es verificar la manera en que se ha venido desarrollando el procedimiento analizado.
- El **resultado** será los indicadores existentes hasta el momento del procedimiento que se está analizando.

4.3.4 Identificar y relacionar según ISO 27002 y COBIT

- El **objetivo** es relacionar el procedimiento con el dominio y objetivo de control correspondiente según la norma ISO 27002 y COBIT
- El **resultado** será la descripción del control y las guías de seguridad.

4.3.5 Cuadro resumen de la etapa

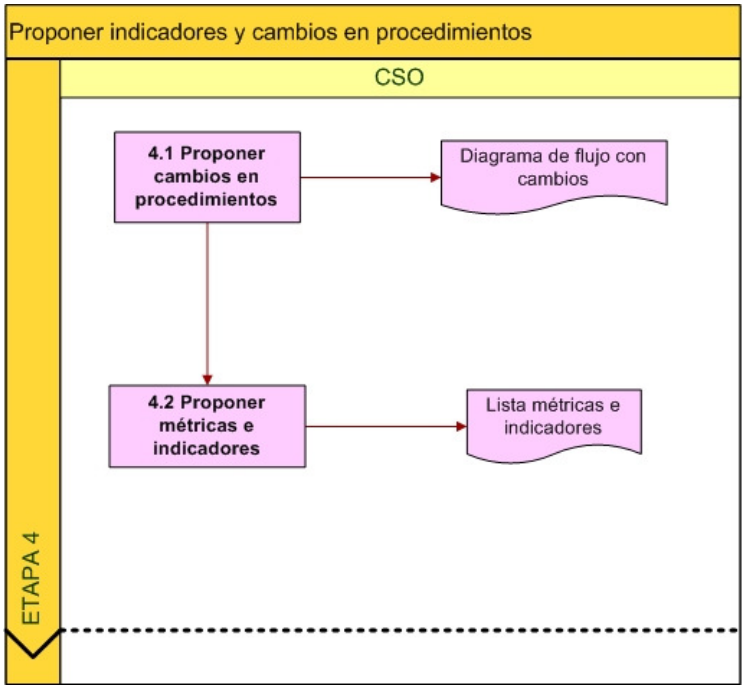
Tabla 7: Etapa 3: Objetivos y Resultados - Metodología de Investigación

OBJETIVO	RESULTADO
Conocer relevancia de los procedimientos de SI en el sistema de gestión a evaluar.	Cuadro de ponderación de importancia de procedimientos.
Conocer relación entre actores, tareas y documentos del proceso a evaluar.	Resumen y breve explicación de las tareas incluidas dentro del procedimiento a evaluar. Diagramas de flujo del proceso a evaluar, identificando actores y tareas.
Conocer los resultados del procedimiento hasta antes del inicio de la evaluación.	Gráfica de métricas e indicadores existentes. Cuadro de cumplimiento de procedimiento en la empresa.
Relacionar procedimiento a evaluar con los modelos de gestión a usar	Descripción de controles relacionados y guías de seguridad.

Fuente: Elaboración Propia

4.4 4ta. Etapa: Proponer indicadores y cambios en procedimientos

Figura 16. Metodología: Etapa 4



Fuente: Elaboración propia

4.4.1 Proponer cambios en procedimientos

- El **objetivo** es evaluar los procesos propuestos, determinar las modificaciones y determinar las acciones necesarias para la implementación tomando como base los controles planteados en la norma ISO 27002.
- El **resultado** será la descripción del procedimiento modificado, el diagrama de flujo del mismo y las acciones propuestas para la implementación.

4.4.2 Proponer indicadores

- El **objetivo** es proponer los indicadores que sirvan para un mejor desarrollo y gestión de la información manejada tomando como base la norma COBIT
- El **resultado** serán los indicadores propuestos desarrollados a partir de la modificación del procedimiento.

4.4.3 Cuadro resumen de la etapa

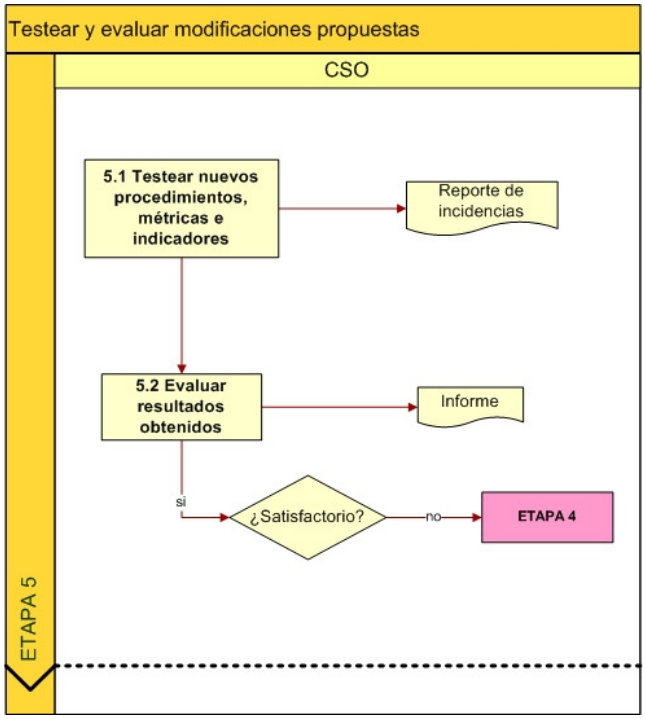
Tabla 8: Etapa 4: Objetivos y Resultados - Metodología de Investigación

OBJETIVO	RESULTADO
Evaluar los procesos propuestos y determinar las modificaciones a realizar.	Procedimiento modificado plasmado en documento FDM Acciones necesarias para implementar nuevo procedimiento. Diagrama de flujo modificado.
Proponer indicadores en base a las modificaciones planteadas.	Indicadores propuestos descritos en documento FDM

Fuente: Elaboración Propia

4.5 5ta. Etapa: Testear y evaluar modificaciones propuestas

Figura 17. Metodología. Etapa 5



Fuente: Elaboración propia

4.5.1 Testear nuevos procedimientos e indicadores.

- El **objetivo** es determinar la efectividad de los nuevos procedimientos y de los indicadores y métricas derivados de estos, los cuales han sido implementados en el Sistema de Gestión en un ambiente real.
- El **resultado** será un reporte indicando las incidencias ocurridas durante la etapa de testeo las cuáles serán reportadas por el personal encargado de las pruebas.

4.5.2 Evaluar resultados obtenidos de procedimientos e indicadores.

- El **objetivo** es facilitar la toma de decisiones a la Gerencia responsable, tomando com base el reporte obtenido, quien determinará si el procedimientos es aplicable.
- El **resultado** será un informe en donde se detallen todas las ventajas y desventajas que se obtienen después de la aplicación del procedimiento, asi como las diferencias halladas en indicadores.

4.5.3 Cuadro resumen de la etapa

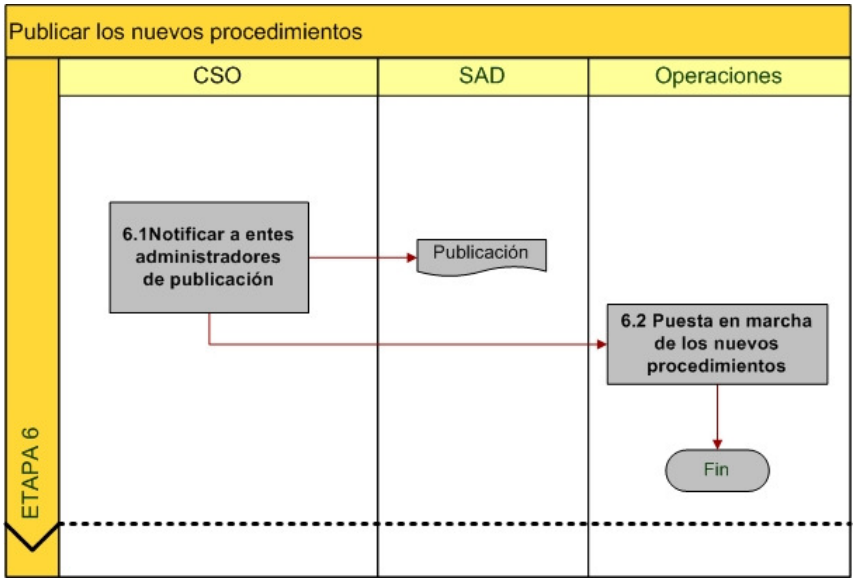
Tabla 9: Etapa 5: Objetivos y Resultados - Metodología de Investigación

OBJETIVO	RESULTADO
Determinar la efectividad de los nuevos procedimientos y de los indicadores y métricas	Reporte de incidencias durante ejecución de procedimiento.
Facilitar la toma de decisiones a la Gerencia para determinar aplicación de procedimiento.	Informe de ventajas y desventajas halladas. Tabla de comparación entre indicadores y métricas.

Fuente: Elaboración Propia

4.6 6ta. Etapa: Publicar los nuevos procedimientos

Figura 18. Metodología: Etapa 6



Fuente: Elaboración propia

4.6.1 Notificar a entes administradores de publicación de documentación

- El **objetivo** es dar a conocer el nuevo procedimiento al personal involucrado, el cual ha sido validado por la Gerencia responsable mediante su publicación en el sistema de documentación de la organización.
- El **resultado** será la publicación del nuevo procedimiento en el sistema de documentación de la organización.

4.6.2 Puesta en marcha de los nuevos procedimientos

En esta etapa todos aquellos procedimientos validados por la gerencia se pondrán en funcionamiento.

4.6.3 Cuadro resumen de la etapa

Tabla 10: Etapa 6: Objetivos y Resultados - Metodología de Investigación

OBJETIVO	RESULTADO
Dar a conocer el nuevo procedimiento al personal involucrado.	Publicación del nuevo procedimiento en el sistema de administración de documentación

Fuente: Elaboración Propia

Capítulo 5: DESCRIPCIÓN DE LA EMPRESA EN ESTUDIO

5.1 Descripción de PetroAmérica:

Desde su creación en 1953 PetroAmérica ha sido una empresa pionera en la industria del petróleo. Actualmente es la mayor compañía de Brasil, la segunda productora de petróleo en Argentina y la tercera compañía industrial más grande de Latinoamérica.

Al ser una empresa totalmente integrada, PetroAmérica interviene en varias áreas de la actividad petrolera incluyendo:

- Exploración y producción de petróleo y gas natural
- Refinación, comercialización y transporte de petróleo y sus derivados
- Petroquímica y generación de energía

Al tener más de 50 años en el negocio de exploración y producción de petróleo, PetroAmérica es hoy una de las 12 principales empresas productoras de petróleo a nivel mundial.

5.2 Misión, Visión y Valores

5.2.1 Misión

Actuar en forma segura, rentable e integrada, con responsabilidad social y ambiental, en las actividades de la industria del petróleo, el gas y la energía, para ofrecer productos y servicios adecuados a las necesidades de los clientes, contribuyendo al desarrollo de la gente y de los países donde actúa.

5.2.2 Visión

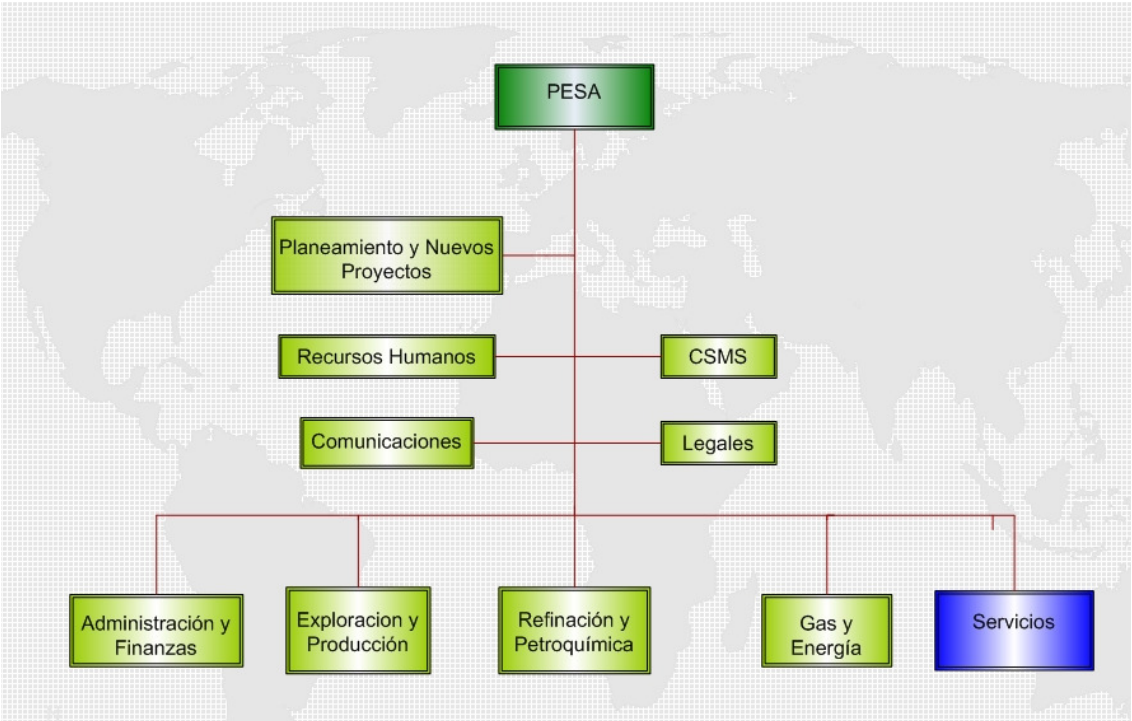
Ser una empresa integrada de energía, con fuerte presencia internacional, actuando con foco en la rentabilidad y en la responsabilidad social y ambiental.

5.3 Organigrama

PetroAmérica al ser una empresa transnacional tiene una organización similar replicada en las filiales, en los que se puede observar el nivel en el que se encuentra la Unidad TI – SIC (Tecnología Informática – Servicios Informáticos y Comunicaciones),

responsable de evaluar los procedimientos y procesos para iniciar el proyecto de Elaboración y formalización del SGSI dentro del área de Tecnología Informática.

Figura 19: Organigrama Principal PetroAmérica



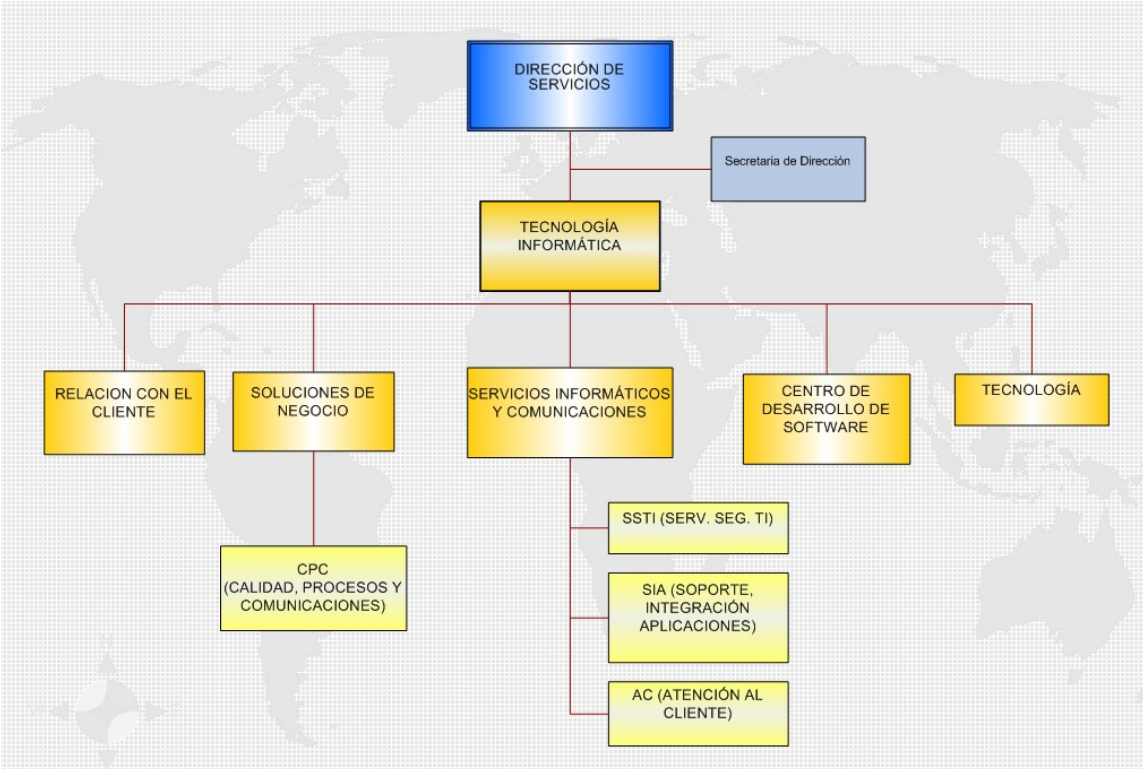
Fuente: Elaboración propia

El área de TI tiene como misión acompañar a los clientes en la integración, el crecimiento y la diferenciación de la empresa, brindándoles soluciones de TI y de soporte a los procesos de negocios:

- Integración: Integrar negocios, procesos, culturas, a lo largo de la cadena de valor extendida, alineados con las políticas y directrices corporativas de gestión, seguridad, medio ambiente y salud.
- Crecimiento: Acompañar los planes de negocio de la Compañía.
- Diferenciación: Sumar ventajas competitivas. Identificar las expectativas de los Clientes para poder entregar una solución que los fidelice.

Por otro lado, el propósito de SIC (dentro de TI) durante la implementación y a lo largo de todo el ciclo de vida de las soluciones informáticas, es ocuparse de realizar todas las actividades necesarias para controlar que ellas brindan los resultados para los cuales fueron creadas y en las condiciones pactadas en los Acuerdos de Servicios.

Figura 20: Organigrama De Dirección de Servicios - PetroAmérica



Fuente: Elaboración propia

5.4 SAD: Herramienta de estandarización

El Sistema de estandarización es un instrumento de gestión de PetroAmérica, además constituye un sistema clave de apoyo a los sistemas de gestión.

El SAD es un sistema integrado, desarrollado por PetroAmérica bajo el ambiente Lotus Notes, el cual permite gerenciar todo el flujo de estandarización en PetroAmérica. Este sistema es alimentado de manera descentralizada.

SAD asigna códigos de identificación de estándares y contiene información estadística de todos los estándares Activos, en Elaboración, en Aprobación, en Implantación, Revisados o Cancelados.

Los estándares están organizados en Bases de Datos separadas de acuerdo al origen de los mismos con el objeto de atender en forma simultánea las necesidades de integración y facilidad de uso.

5.5 El SGC en la Empresa y su relación con la Seguridad de la Información.

La política de calidad de PetroAmérica asume para sus empresas controladas y/u operadas, en dicho país y en el exterior, el compromiso de suministrar productos y servicios de calidad, con un estilo innovador, y creativo de gestión, con foco en sus clientes, la responsabilidad social. Ejerce sus actividades de manera ética, valoriza el liderazgo en cuestiones de Salud, Seguridad y Medio Ambiente, y asume los siguientes compromisos que constituyen su Política de Calidad:

CLIENTES: satisfacer los requisitos de nuestros clientes de una manera competitiva y rentable, evaluando sistemáticamente su grado de satisfacción, identificando sus necesidades y expectativas y mejorando la calidad de nuestros productos y servicios.

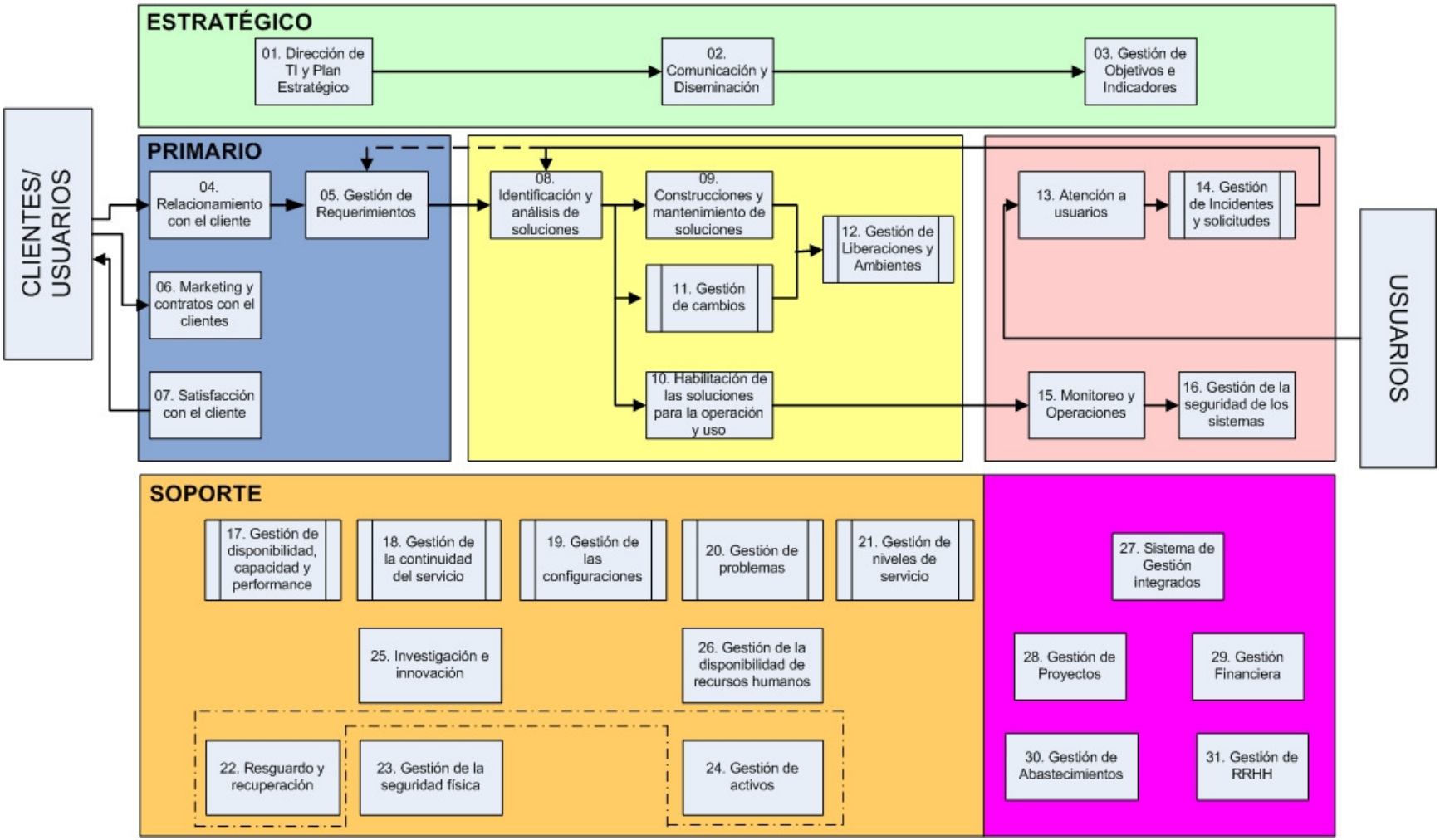
PERSONAS: valorizar a las personas de la organización procurando su desarrollo y promoviendo su participación creativa en equipos de trabajo, en un ambiente propicio que permita mejorar la productividad y la calidad de vida.

PROVEEDORES: calificar, evaluar y desarrollar a nuestros proveedores clave para que adopten estándares de trabajo acordes con nuestra Política de Calidad.

GESTIÓN: implementar sistemas de gestión integrados, evaluarlos sistemáticamente y establecer objetivos alineados con los empresariales, con el fin de mejorar en forma continua los procesos y resultados.

En la siguiente figura, observaremos el Mapa de Procesos con los que actualmente cuenta el Sistema de Gestión a evaluar: Genéricos, Primarios y de Soporte.

Figura 21. Procesos del SGC



Fuente: Elaboración Propia

Capítulo 6: APLICACIÓN DE LA METODOLOGÍA

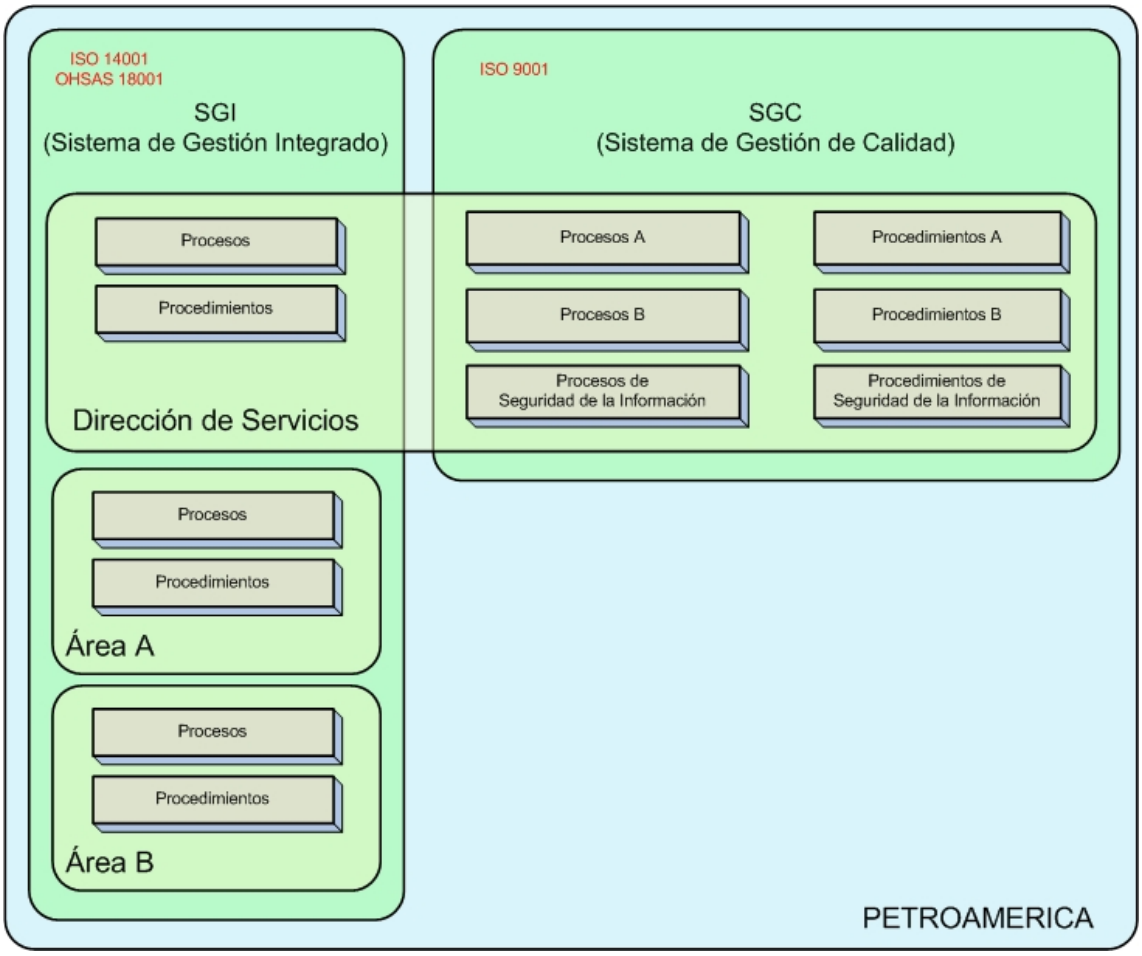
Una vez definida la metodología de trabajo así como las herramientas (teóricas y prácticas) a usar, se procederá a desarrollar etapa por etapa el estudio

6.1 Estructura del Sistema de Gestión

6.1.1 Estudio de estructura de procesos y procedimientos

Si bien el área de Dirección de Servicios de la empresa PetroAmérica tiene ya implementado un Sistema de Gestión de Calidad basada en las normas ISO 9001 también tiene como objetivo dentro de su Plan Estratégico el incidir en aquellos temas que involucren y puedan afectar la integridad de información que esta maneja.

Figura 22. Estructura de Sistemas de Gestión actuales.



Fuente: Elaboración propia

Para lograr su cometido, se ha planteado en primera instancia realizar revisiones y modificaciones en aquellos procedimientos que forman parte del SGC pero que a su vez también cumplan con los requerimientos de la seguridad de la información, es decir, todos aquellos procesos que ya estén ejecutándose y a los cuales se les puede evaluar para medir el nivel de madurez en la que se encuentran.

6.1.2 Modificación de procesos y procedimientos.

Por otro lado, la modificación de procesos tiene también un procedimiento a seguir, en el que se involucran diversas personas de la compañía, cuyo principal trabajo es asegurar el cumplimiento de las normas para la publicación y ejecución de las innovaciones o creaciones que afecten el desarrollo de las operaciones.

6.1.2.1 Actividades

- Detectar la necesidad: Cualquier colaborador de TI que utiliza un proceso puede detectar la necesidad de una modificación del mapa, la que comunicará al Referente de Calidad de su área
- Solicitar la modificación: El Referente de Calidad recibe la solicitud y propone una modificación concreta al responsable de dicho proceso.
- Validar y definir equipo responsable: El Responsable del Proceso valida dicha necesidad y forma un equipo para su diseño e implementación. Comunica al GP la modificación para su revisión.
- Revisar la solicitud: El Grupo de Práctica (GP) analiza la solicitud y la naturaleza del cambio solicitado realizando además las siguientes tareas.
- Identificar el proceso dentro del Mapa de Procesos
- Planificar la modificación: El GP junto con el Responsable, realizan un plan para la implementación de la incorporación o modificación del estándar.
- Diseñar la modificación: El GP diseña la modificación y arma un plan de implantación, comunicación y si corresponde de capacitación.
- Homologar el cambio: El Responsable del Proceso junto con el Equipo Responsable del desarrollo homologa el cambio con el soporte del GP y la participación de los afectados en las modificaciones.
- Aprobar y Publicar: El Aprobador del proceso lo aprueba, con lo cual el mismo se puede publicar.
- Implantar y Comunicar: El Equipo Responsable realiza la implantación del proceso y la comunicación a todos los involucrados.

Figura 23. Modificación de procesos y procedimientos

Fuente: Elaboración propia

6.2 Análisis de Estado actual

6.2.1 Distribución de Procesos y Procedimientos

De acuerdo a los procesos existentes y definidos en la Dirección de Servicios, observamos que la mayoría de estos (estratégicos, primarios o de soporte) tiene asociado uno o más procedimientos / estándares validados y publicados en el SAD, además de pertenecer a un Macroproceso.

A través del cuadro adjunto, se pretende dar una visión global de los procesos existentes en la empresa y así tomar aquellos que representen un punto crítico para la Gestión de la Seguridad de la Información.

Tabla 11. Procesos del Sistema de Gestión a Evaluar

Tipo Proceso	Macroproceso	N° Proceso	Estándares / Procedimientos de SAD
Estratégico	….	….	….
Primario (Relación con el Cliente)	….	….	….
Primario (Diseño - Construcción)	….	….	….
Primario (Operaciones)	….	….	….
Soporte (internos)	Gestión de la Continuidad del Servicio	18	Plan de recuperación de servicios de CPD por desastre
	Gestión de las Configuraciones	19	*Sin procedimiento asociado*
	Gestión de Problemas	20	*Sin procedimiento asociado*
	Gestión de Niveles de Servicios	21	*Sin procedimiento asociado*
	Resguardo y Recuperación	22	Recuperación y Resguardo por Contingencia
	Gestión de la Seguridad Física	23	Infraestructura y Arquitectura Técnica de TI
	Gestión de Activos	24	Baja Física de Equipamiento
		24	Inventario de Hardware
		24	Inventario de Software
	Gestión de Disponibilidad de RRHH	26	*Sin procedimiento asociado*
Soporte (externos)	….	….	….

Fuente: Elaboración Propia

6.2.2 Análisis GAP

Para presentar el resumen de resultados, se ha tomado en cuenta las brechas identificadas entre las normas ISO 27002 y los controles administrativos documentados e implementados.

En la tabla a continuación se presenta un resumen que indica la cantidad de controles que se encuentran cubiertos de forma total, parcial o sin cobertura respecto al sistema de Gestión de la empresa, agrupado por cada uno de los 11 dominios de la ISO 27002.

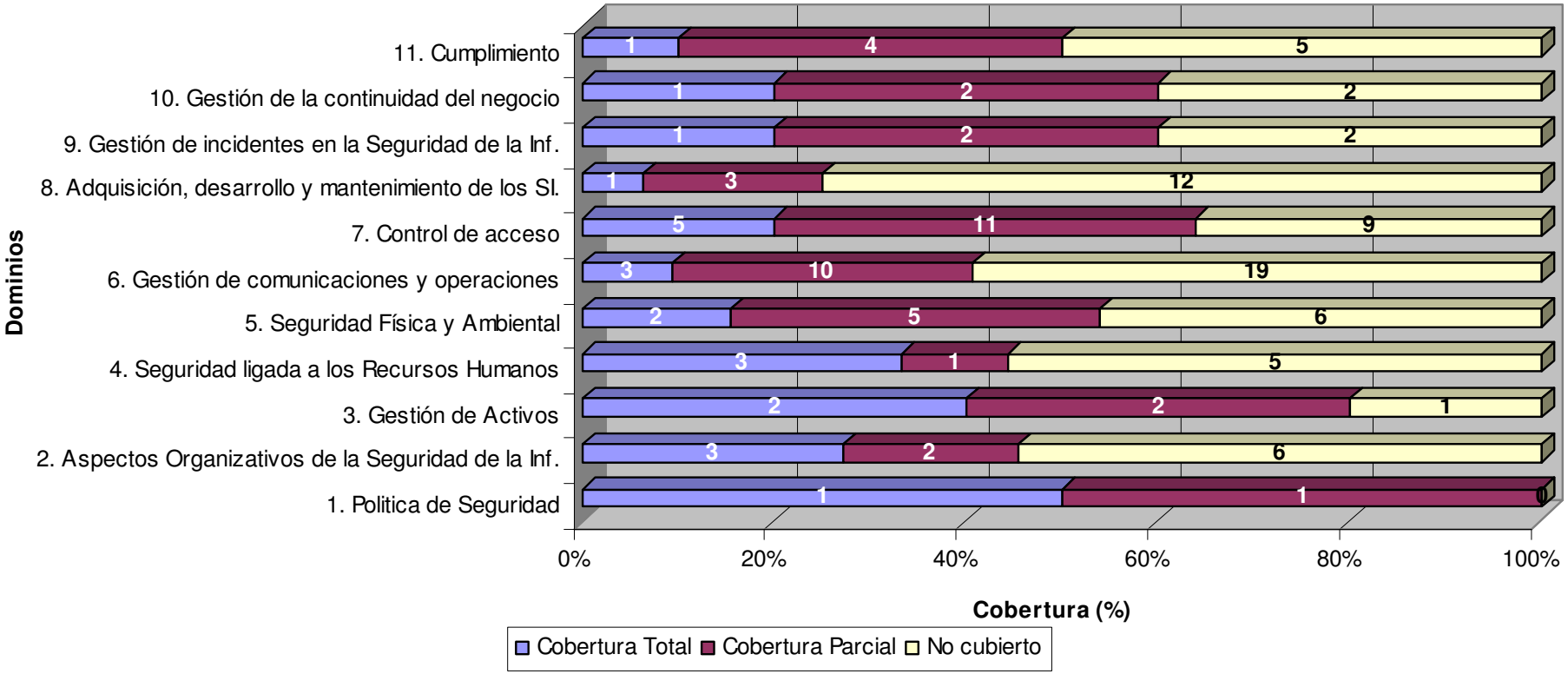
Tabla 12. Cobertura de controles en Sistema de Gestión actual

Dominio	Cobertura Total	Cobertura Parcial	No cubierto	Total
1. Política de Seguridad	1	1	0	**2**
2. Aspectos Organizativos de la Seguridad de la Inf.	3	2	6	**11**
3. Gestión de Activos	2	2	1	**5**
4. Seguridad ligada a los Recursos Humanos	3	1	5	**9**
5. Seguridad Física y Ambiental	2	5	6	**13**
6. Gestión de comunicaciones y operaciones	3	10	19	**32**
7. Control de acceso	5	11	9	**25**
8. Adquisición, desarrollo y mantenimiento de los SI.	1	3	12	**16**
9. Gestión de incidentes en la Seguridad de la Inf.	1	2	2	**5**
10. Gestión de la continuidad del negocio	1	2	2	**5**
11. Cumplimiento	1	4	5	**10**
Total	23	43	67	**133**

Fuente: Elaboración propia

A continuación se muestra un gráfico comparativo entre la cantidad de controles definidos en cada uno de los 11 dominios de ISO 27002 y la cantidad de controles que son soportados actualmente por el SGC.

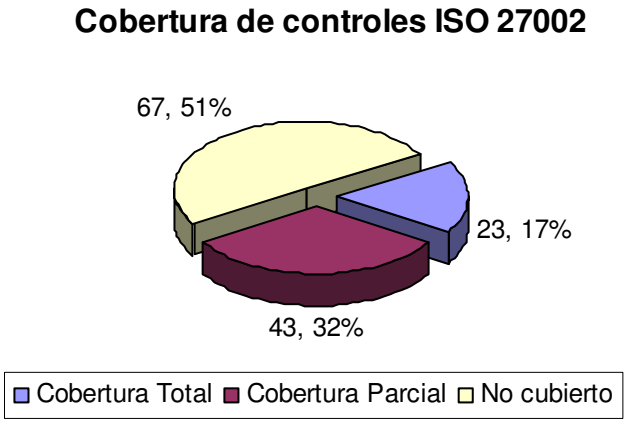
Figura 24. Estado de cobertura de controles de ISO 27002 por Dominios



Fuente: Elaboración propia

En el siguiente gráfico se puede apreciar el porcentaje de controles que proponen las normas ISO y que pueden ser soportados de una manera total o parcial por la situación actual de seguridad de la empresa PetroAmérica

Figura 25. Porcentaje de Tipo de Cobertura de Controles ISO 27002



Fuente: Elaboración propia

6.3 Identificación y descripción de Procedimientos

En el universo de procedimientos existentes dentro del SAD de la empresa en estudio debido a no contar con el tiempo necesario nos enfocaremos solamente en el proceso de Recuperación y resguardo por Contingencia de Datos almacenados en Servidores.

6.3.1 Identificación los procedimientos y procesos críticos

A través de un cuadro de ponderación se definirán el orden de importancia y/o criticidad de los procedimientos existentes relacionados a la seguridad. Se tomarán en cuenta los siguientes criterios:

Tabla 13: Criterios de ponderación de procedimientos a evaluar.

	VALOR			
CRITERIOS	1	2	3	4
Frecuencia de Ejecución	A pedido	Anual	Mensual	Diaria / Semanal
Frecuencia de Monitoreo	A pedido	Anual	Mensual	Diaria / Semanal
Existencia de Indicadores	Mas de 5 indicadores	Entre 3 y 4 indicadores	Entre 1 y 2 indicadores	Ninguno
Existencia de manuales asociados	Ninguno	Entre 1 y 2 manuales	Entre 3 y 4 manuales	Mas de 5 manuales

Objetivo asociado en ISO 27002	Ninguno	Un objetivo asociado	2 objetivos asociados	3 o más objetivos asociados
Objetivo asociado en COBIT	Ninguno	Un objetivo asociado	2 objetivos asociados	3 o más objetivos asociados

Fuente: Elaboración propia

- Frecuencia de ejecución

  Este criterio nos indicará la frecuencia para la elaboración de los registros solicitados en el proceso. A mayor frecuencia, mayor es la necesidad de control del proceso; por lo tanto, este debería estar dentro de los procesos críticos a evaluar.

- Frecuencia de monitoreo:

  Nos indica la frecuencia en la que el proceso es monitoreado para comprobar la correcta realización de este, sin importar si los resultados obtenidos son los correctos. En ocasiones es similar a la frecuencia de ejecución. Depende también de las programaciones de auditorias internas y externas a la que es sometida el área.

- Existencia de indicadores

  Este criterio nos dará una muestra del estado de control del proceso a través de indicadores. Si estos no existen, la prioridad de la evaluación y cambio será alta, ya que el objetivo principal es justamente crear indicadores para tener un control permanente y ayudar a la toma de decisiones. Esta necesidad se reduce conforme se van elevando la cantidad de indicadores existentes.

- Existencia de manuales asociados

  A través de este criterio se verifica la existencia de algún otro tipo de documentación que sirva para el afianzamiento del proceso, ya sea como un anexo o adjuntándose en alguna parte de la estructura. Por ejemplo, la Norma de Copias de Respaldo y Restauración podría formar parte del proceso de Resguardo y Recuperación por contingencia, figurando como un documento complementario o, según se detecte en el análisis, siendo eliminada y su contenido considerado y adaptado al proceso final.

- Existencia de objetivos asociados con ISO27002

  Este criterio se basa en la importancia de tener una referencia en los modelos de gestión usados para evaluar adecuadamente el proceso. En este caso este criterio se enfoca en los objetivos de control existentes en la ISO 27002. De existir más objetivos o controles asociados, se incrementará la probabilidad de análisis del

proceso y la prioridad que tendrá este dentro del objetivo final de la creación del SGSI.

- Existencia de objetivos asociados con COBIT
  Similar al criterio anterior pero enfocado a los objetivos planteados por COBIT.

Tabla 14: Resultados de ponderación de Procedimientos críticos

Procedimiento / Estándares a evaluar	Frecuencia de Ejecución	Frecuencia de Monitoreo	Existencia de Indicadores	Existencia de manuales asociados	Objetivos asociados en ISO 27002	Objetivos asociados en COBIT
Nivel de Importancia	**25%**	**25%**	**25%**	**5%**	**10%**	**10%**
Plan de recuperación de servicios de CPD	1	1	4	2	2	3
Recuperación y Resguardo por Contingencia	4	4	3	4	2	2
Infraestructura y Arquitectura Técnica de TI	3	2	2	2	2	2
Baja Física de Equipamiento	1	3	3	2	2	2
Inventario de Hardware	2	3	3	3	2	2

Fuente: Elaboración propia

Como se puede observar a través de la tabla anterior, los procedimientos según el orden a evaluar son los siguientes:

Tabla 15. Procedimiento / Estándares a evaluar

Procedimiento / Estándares a evaluar	Total
Nivel de Importancia	**100%**
Recuperación y Resguardo por Contingencia	**3.35**
Inventario de Hardware	2.55
Infraestructura y Arquitectura Técnica de TI	2.25
Baja Física de Equipamiento	2.25
Plan de recuperación de servicios de CPD	2.10

Fuente: Elaboración propia

6.3.2 Descripción de procedimiento elegido

Resguardo y Recuperación por Contingencia

Este procedimiento divide claramente dos etapas: El resguardo o backup de información y la restauración o recuperación de información.

- **Resguardo**

  Los procesos de resguardo se basa en:
  GESTIÓN: Revisión del requerimiento, consulta con otras áreas de TI, rechazo en caso de no corresponder (por ejemplo, backups no programados de PC's)
  PLANIFICACIÓN: Actualización en la herramienta y/o control que corresponda, generación de la tarea.

  Periodicidad: Para minimizar el impacto sobre el rendimiento se han establecido ciertas reglas sobre la ejecución de backups:
  Backups diarios – diferenciales - ventana de backup 12 hrs.
  Backups semanales – full – ventana de backup 48 hrs.
  Backups mensuales – full – ventana de backup 48 hrs.
  Backups trimestrales – full – ventana de backup 48 hrs.
  Backups anuales – full – ventana de backup 48 hrs.

  Evidencia: Los datos de horarios de comienzo, fin y el tipo de finalización por grupo de backup deben ser registrados diariamente en el parte diario enviado a Operaciones.

  Datos a resguardar: El software Operativo, perfiles de usuario y las configuraciones deberán ser resguardados con el sistema operativo de tal manera que se pueda obtener la integridad de los datos en la recuperación de la información.

  Asimismo, este procedimiento cubre toda la data contenida en los servidores en donde se guarde toda la información privada de la empresa, generada por los trabajadores según los permisos de acceso otorgados de acuerdo a su rango y área y que, por políticas de la organización, no deben ser guardadas en los discos locales de las PC's asignadas.

  Si por requerimientos del negocio, existiera un servidor, cuyos datos no deban seguir el régimen de backup indicado en este estándar, deberá existir en poder

del responsable del sitio, un correo donde el área encargada y el cliente, estén de acuerdo con esta práctica.

Administración e Integridad de los resguardos: Los medios de almacenamiento externo que se obtengan del resguardo mensual/semanal full y sus juegos diferenciales/incrementales diarios, permanecerán en una ignifuga para conservar la integridad de los datos en caso de cualquier tipo de siniestro, fuera del CPD. Además se deberá acompañar el backup de la base de datos del sistema de backup (si corresponde), para su recuperación.

Si el hardware, el software y el tiempo lo permiten, se pueden efectuar copias de los medios de almacenamiento externo, para mayor seguridad, estos deben tener el mismo tratamiento que los originales.

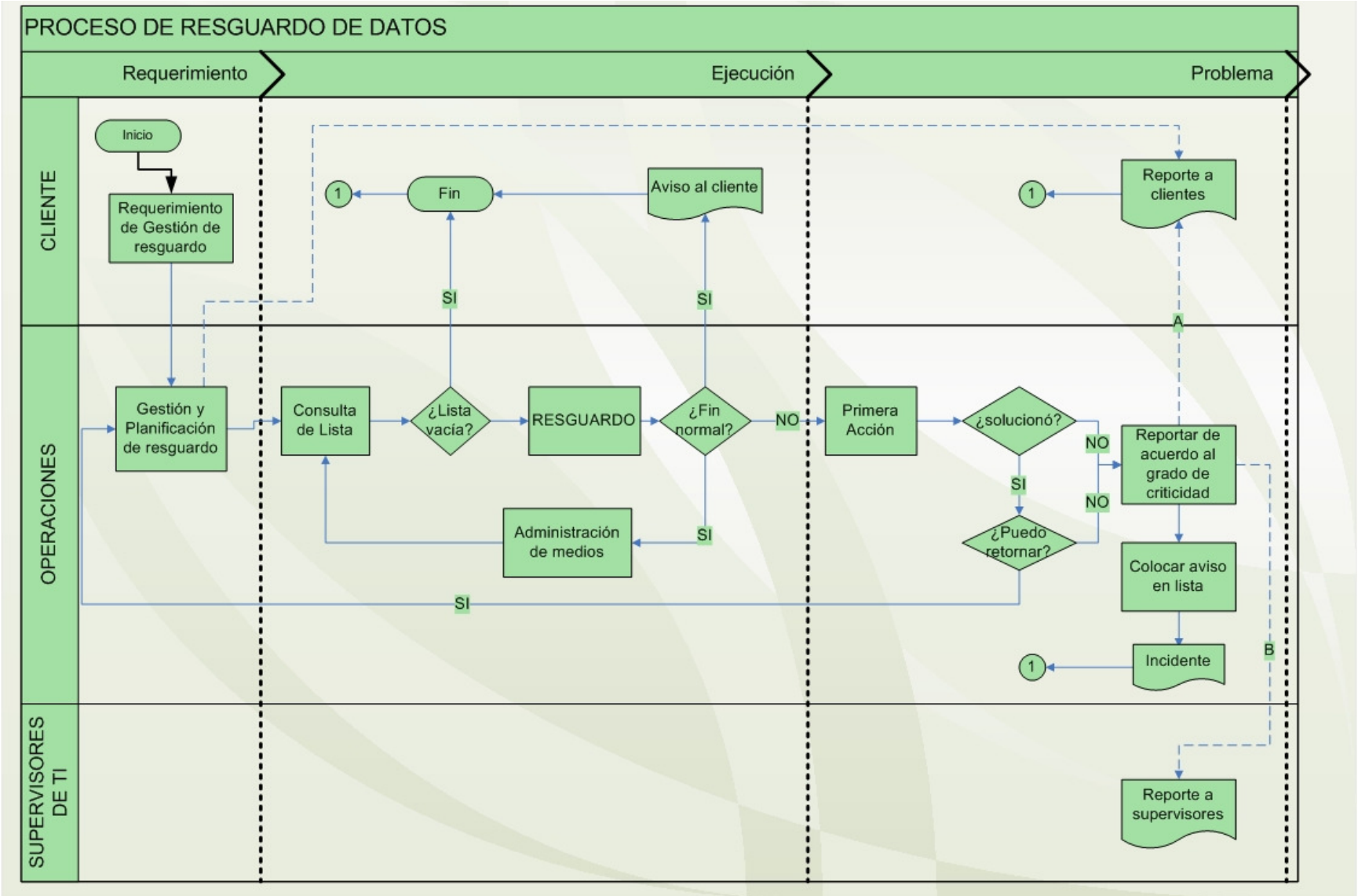
Los medios de almacenamiento externo deberán estar numerados externamente (código de barras, numeración registrada en herramienta de backup o numeración por formulario), además de estar identificados en forma interna. Se deberán administrar los resguardos con algún software que permita realizar reportes sobre los medios, de no contar con él, se deberán administrar manualmente de acuerdo al registro "numeración de los resguardos".

Numeración de resguardos: La numeración de los resguardos se rige a los siguientes parámetros:

- Diarias: DDSIssnn,
  donde DD = LU, MA, MI, JU y nn = rango a utilizar del 1 al 20
- Semanales : SxSIssnn,
  donde Sx = S1, S2, S3, S4 y nn = rango a utilizar del 21 al 40
- Mensuales: MxSIssnn ,
  donde Mx = M1, M2 y nn = rango a utilizar del 41 al 50
- Trimestrales: TxSIssn,
  donde Tx = T1, T2, T3 y nn = rango a utilizar del 51 al 70
- Anuales: AxSIssnn,
  donde AX = A1, A2, A3, A4, A5 y nn = rango a utilizar del 71 al 90

  y donde, para todos: SI: sitio, ss: nro. Identificador de servidor.

Figura 26. Proceso de Resguardo de Datos



Fuente: Elaboración propia

- **Recuperación:**

GESTIÓN Y PLANIFICACIÓN: Disposición de los recursos necesarios para la recuperación (Software instalado en servidor, librería de medios disponible o unidad de cinta, espacio suficiente, operador, etc.)

Periodicidad: Las recuperaciones son realizadas a pedido, es decir, según la necesidad del usuario, quien para solicitar el servicio debe especificar el archivo o los archivos necesitados así como la fecha solicitada de restauración.

Evidencia: Los datos de horarios de comienzo, fin y el tipo de finalización por grupo de backup deben ser registrados diariamente en el parte diario enviado a Operaciones.

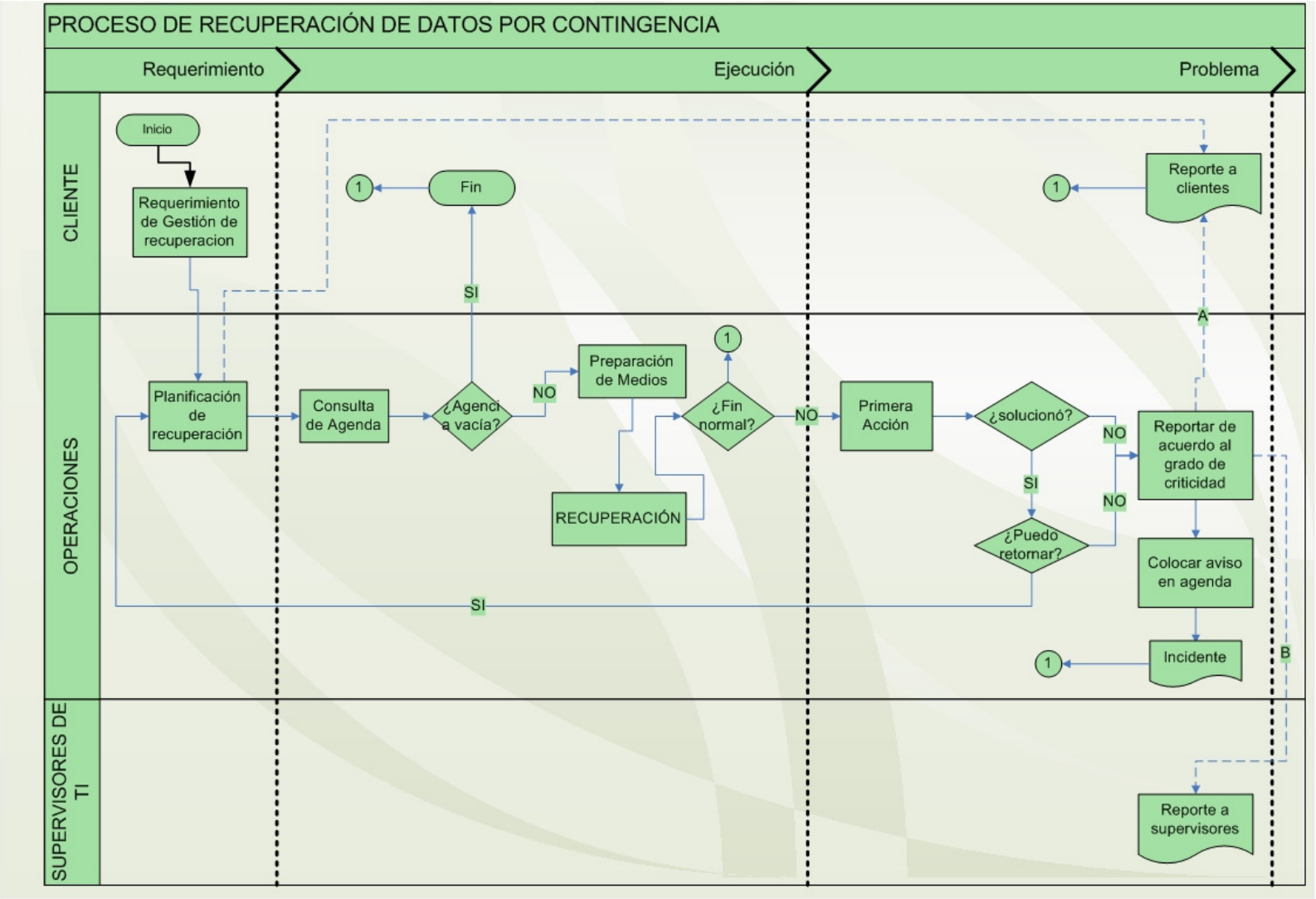
La información Operativa, los logs del sistema y los logs aplicativos, deben ser recuperados como copias, en caso que la recuperación sea parcial (a pedido del usuario). Si la recuperación se realiza en forma total (recuperación de todo el servidor), se deberá utilizar primero el resguardo del software operativo, el software de aplicación (puede ser utilizado el software original), las configuraciones, luego toda la información operativa y los diferentes logs de ser necesario.

Pruebas de integridad y Recuperación: Para asegurar que el backup realizado asegure la integridad de los datos se realizan pruebas, cuyo monitoreo es trimestral. Estas verificaciones y restores pueden ser solicitadas por los usuarios pero en caso de no estar cubierta la totalidad de cintas en el periodo del año se deberá realizar pruebas de recuperación

La prueba consiste en:

- Retirar de la caja ignifuga un backup full mensual, trimestral o anual del servidor que contenga las aplicaciones y/o documentos críticos
- Realizar una verificación en el software, guardar la evidencia y registrar en el formulario “Prueba de Recuperación” la fecha, el servidor probado, y el resultado. Guardar el formulario en la caja ignifuga.
- Esta operación se repetirá mensualmente hasta tener probado todo el ciclo de backups, una vez finalizado el ciclo, se repite la prueba mensual desde el principio.

Figura 27. Proceso de Recuperación de Datos



Fuente: Elaboración propia

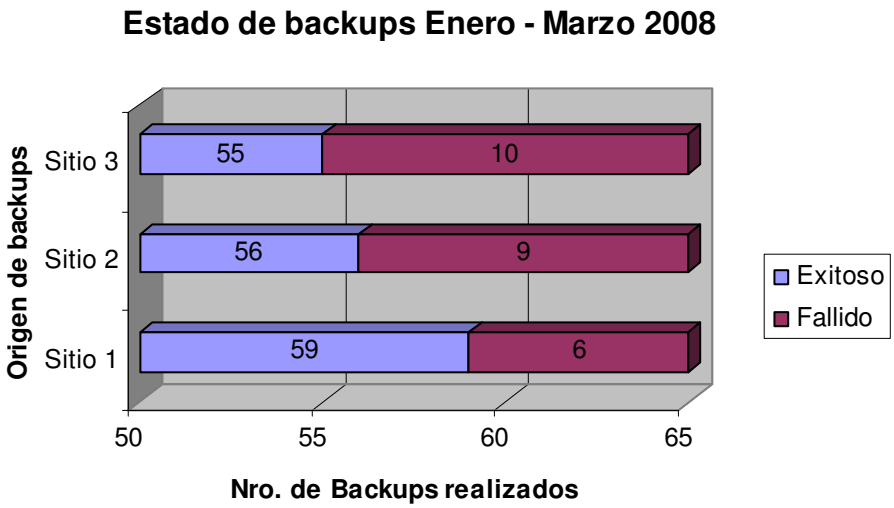
6.3.3 Resultados de proceso actual

- **Resguardo**

Actualmente, el proceso de Resguardo de la Información se realiza con normalidad no presentándose problemas constantes. En el caso de los hechos aislados, estos son reportados a través de un Parte Diario al área de TI - Argentina.

En el siguiente gráfico podremos observar el porcentaje de resguardos que presentaron problemas durante los meses de Enero a Marzo del año 2008, en las diversas locaciones de la empresa en Perú. Hay que resaltar que este gráfico es resultado de la compilación de data basada en los logs generados por la herramienta de respaldo utilizada.

Figura 28. Estado de Backups Enero – Marzo 2008



Fuente: Elaboración propia

Esta muestra se tomó durante las 13 primeras semanas de backups, es decir, 65 días en donde se realizó la tarea de resguardo programada entre backups diarios, semanales, mensuales y una tarea trimestral. Como podemos observar en el Sitio 1 sólo se registraron 6 backups fallidos siendo esto el 10.17% del total de resguardos. De igual manera en los sitios 2 y 3, se registraron errores en 16.07% y 18.18% del total de resguardos respectivamente.

Aun cuando estas cifras fueron elevadas, no se tomaron las acciones correctivas necesarias, lo cual se vio reflejado en el siguiente trimestre en el que los resultados

fueron similares. Debido a esto se optó por analizar, realizar y plantear cambios en los procedimientos seguidos hasta ese momento así como buscar las herramientas que permitan monitorear de un modo constante la eficacia del proceso.

- **Restores**

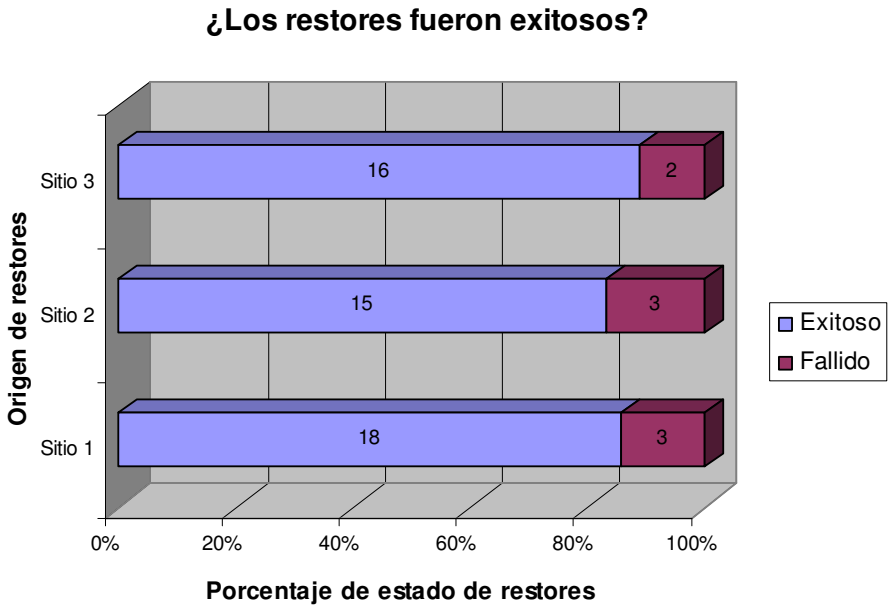
En el siguiente gráfico se muestra la cantidad de restauraciones programadas por sitio realizados a las cintas críticas (anuales, trimestrales. mensuales) durante un año, independientemente de sus resultados. Como observamos de un total de 30 restauraciones críticos que se debían haber hecho en los 3 sitios (10 restauraciones por sitio), sólo se realizaron 18 durante el 2008. Con esto se concluye que no hay un control total sobre la comprobación del backup realizado y la integridad de la información que se pueda restaurar.

Figura 29. Restores críticos realizados en el año 2008

Fuente: Elaboración propia

De los restores realizados durante el periodo de tiempo ya mencionado, se puede observar que en dos de los sitios se presentó un fallo en la integridad de los datos.

Figura 30. Resultado de restores - 2008



Fuente: Elaboración propia

Esto nos demuestra que, "probablemente" no hubo una correcta verificación de la integridad de los datos en esas cintas una vez acabado el respaldo correspondiente. La verificación de la data una vez respaldada es una práctica recomendada más no establecida dentro del procedimiento, otro punto más a tomar en cuenta dentro de los cambios propuestos.

6.3.4 Identificación y relación según ISO 27002

Tomando como base los objetivos de control de ISO 27002 se presenta la siguiente relación entre estos y el proceso al cual se enfoca el presente trabajo.
Se realizó un análisis del estado actual del procedimiento contra las recomendaciones realizadas por la norma, encontrándose falencias, signadas en el presente trabajo como "incidencias".

A. El **objetivo de control 10.5.1** de ISO27002 nos indica que se deben realizar copias de respaldo de la información comercial y software esencial y estas deben ser probadas de forma regular de acuerdo a la política.

De acuerdo al procedimiento actual:

- **Resguardo**

  - Los niveles y frecuencias de recuperación de la información se encuentran establecidos de a cuerdo a las necesidades de la organización.

- Se ha establecido un resguardo temporal (diario) para aquellos servidores con información de alta rotación y usabilidad. Asimismo, como política de la empresa todos los documentos electrónicos trabajados por los usuarios deben ser guardados dentro de las unidades de red seteadas en cada PC y que corresponden a espacios físicos dentro del File Server.
- Los medios de respaldo son resguardados en un lugar seguro (remoto) que evite que pueda sufrir algún daño ante cualquier desastre. En el caso de Lima, estos medios son trasladados hasta las instalaciones de una empresa que brinda el servicio de almacenamiento de medios. En el caso de las dos locaciones en provincia, y debido a la cercanía entre estas, se ha optado por el intercambio de estos medios según se requiera y con un control estricto mediante guías de remisión. Asimismo, se deberá contar con cajas ignífugas para el resguardo.

- **Recuperación**

- ***INCIDENCIA 1A:*** Se realizan restores de manera aleatoria de acuerdo a las necesidades de los usuarios pero no se cumple con la revisión de todos los medios existentes.

  Por lo general, los restores solicitados por usuarios son extraídos de las cintas Diarias, por lo que la disponibilidad de las cintas de menor rotación no es probada con frecuencia.
- ***INCIDENCIA 2A:*** El procedimiento de recuperación deberá ser probado y comprobado regularmente para verificar y asegurar que son eficaces y que pueden recuperarse en el tiempo que ha sido establecido por los procedimientos operativos.

  Actualmente no se tiene establecido un plan de restauraciones que contemple todas las cintas activas, dejando a disposición del área el momento en el que se realizarán las pruebas.
- ***INCIDENCIA 3A****:* Los sistemas críticos en las locaciones al interior poseen un juego de medios de almacenamiento auxiliar (copias mensuales), sin embargo, en Lima no se cuenta con este tipo de precaución.

B. El **objetivo de control 10.7.1** de ISO27002 indica que debemos evitar daños a los activos e interrupciones de las actividades de la organización. Los medios deben ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, modificación, robo u otros

- **Resguardo**
  - ***INCIDENCIA 1B:*** Se realiza el re-etiquetado y/o marcado de aquellos medios magnéticos que sean considerados no necesarios para su posterior reutilización pero no se eliminan los datos allí contenidos.
  - ***INCIDENCIA 2B:*** Se reporta de forma verbal aquellas cintas que dejarán de ser usadas (desechadas o para su reutilización en caso de requerirlas para pruebas). No se lleva un registro de estos medios, almacenándose en un espacio asignado dentro de las instalaciones.
  - Los medios de almacenamiento son resguardados cumpliéndose con las especificaciones de los fabricantes (temperatura, humedad, etc.).
  - Se han identificado todos los medios de almacenamiento se acuerdo a la nomenclatura indicada (véase 6.3.2).
  - En los procedimientos figuran los responsables de la realización de los backups y restores. Además existe una lista manejada por la empresa que provee el servicio de resguardo conteniendo los nombres del personal que puede decepcionar / entregar los medios de almacenamiento usados.

C. El **objetivo de control 10.7.2** de ISO27002 establece procedimientos formales para minimizar el riesgo de filtro de información sensible a personas externas con la eliminación segura de los medios.
Los procedimientos para la seguridad de los medios que contienen información sensible deben ser conmensurados con la sensibilidad de dicha información.

De acuerdo al procedimiento actual:

- **Resguardo**
  - ***INCIDENCIA 1C:*** No se realiza la eliminación de los medios de forma segura cuando son catalogados como inservibles (incinerándolos, triturándolos o vaciando sus datos) de acuerdo a lo tratado en las incidencias 1B y 2B, *Referencia: Incidencia 1B y 2B*
  - La información respaldada abarca toda la data de forma general incluyendo la información crítica

A continuación mostramos la relación entre los objetivos de control de ISO 27002, referidos líneas arriba, y los correspondientes a COBIT, norma con la cual estableceremos los indicadores necesarios para evaluar el procedimiento propuesto.

Tabla 16. Relación entre el objetivo 10.5 de ISO 27002 y COBIT

Objetivos de Control ISO 27002	Áreas ISO 27002	**Objetivos de Control COBIT**	Procesos COBIT
10.5 Backup			
10.5.1 Recuperación de la información	10 Gestión de Comunicaciones y Operaciones	DS11.2 Recuperación de la información	DS11 Administración de la información
		DS11.5 Respaldo y restauración	
		DS11.6 Requerimientos de seguridad para la administración de datos	

Fuente: Isaca.org

Tabla 17. Relación entre el objetivo 10.7 de ISO 27002 y COBIT

Objetivos de Control ISO 27002	Áreas ISO 27002	**Objetivos de Control COBIT**	Procesos COBIT
10.7 Manejo de medios			
10.7.1 Gestión de medios removibles	10 Gestión de Comunicaciones y Operaciones	DS11.2 Acuerdos de almacenamiento y conservación	DS11 Administración de la información
		DS11.3 Sistema de administración de librerías de medios	
		DS11.4 Eliminación	
10.7.2 Eliminación de medios		DS11.3 Sistema de administración de librerías de medios	
		DS11.4 Eliminación	

Fuente: Isaca.org

6.4 Propuesta de indicadores y cambios en procedimientos

6.4.1 Cambios propuestos en procedimientos

De acuerdo a las falencias encontradas (incidencias) se plantean cambios en el procedimiento.

INCIDENCIA 1A: Se plantea que las pruebas de verificación y recuperación de datos de cintas de backup sean llevadas mediante un cronograma específico que abarque la totalidad de cintas críticas y así llevar un control adecuado.

Para tal efecto, se creará el “Plan Anual de Verificación y Recuperación” el mismo que debe asegurar que las pruebas abarquen el total de cintas de backup de todos los sitios que posean las características apropiadas:

- Estar registrada correctamente en el formulario de “Numeración de resguardos” o en el caso de contar con software específico en el inventario de cintas utilizadas.
- Tener duración de resguardo mayor o igual a 90 días.

El Plan deberá ser elaborado durante la 1era semana laborable de cada año.

INCIDENCIA 2A: Debido a que la planilla actual de verificación de restores contiene sólo algunos campos específicos y nada detallados, se ve la necesidad de plantear una nueva planilla de control llamada “Formulario de Pruebas de Verificación y Recuperación Local”, el cual contiene entre otros campos: La cinta y el servidor probado, el archivo recuperado y el número de log proporcionado por la herramienta de respaldo y restauración.
Este archivo será requerido según se cumpla con el Plan Anual de Verificación y recuperación y será guardado en la caja ignífuga junto a las cintas de backup.

INCIDENCIA 3A*:* Se plantea para la sede de Lima, crear un backup a disco que sirva como medio auxiliar ante la pérdida de alguno de los medios magnéticos (cintas), para su posterior pase a un medio de almacenamiento externo. Este backup full auxiliar se tomará cada fin de semana posterior al backup correspondiente y será sobrescrito mensualmente, es decir tendrá un tempo de validez de 4 semanas a partir de la grabación..

INCIDENCIA 1B: Se propone la inutilización de los medios a través de la magnetización, de esta manera, podemos asegurarnos que no se pueda acceder a la información contenida. Este planteamiento deberá formalizarse mediante un procedimiento que toma en cuenta un inventario de medios magnéticos como paso inicial para el control adecuado y permanente.

INCIDENCIA 2B: Se propone crear un registro físico, mediante el cual se reporte al líder de TI el listado de medios desechados, indicando el número físico y lógico del medio. De esta manera se podrá controlar el movimiento de estos modificando el status en el inventario de medios magnéticos.
Estos medios desechados, serán enviados al Centro de Procesamiento de desechos para su respectivo tratamiento una vez al año, previa autorización del CSO, para realizar un adecuado seguimiento y control.

INCIDENCIA 1C: Se subsana de acuerdo a las acciones planteadas para las incidencias 1B y 2B.

A continuación se realiza un resumen de las modificaciones planteadas en el Proceso de resguardo y recuperación, tomando como base las subsanaciones planteadas para las incidencias encontradas.

GESTIÓN Y PLANIFICACIÓN:

GESTIÓN: Revisión del requerimiento de usuarios y requerimientos programados. Registro adecuado de restores programados.
PLANIFICACIÓN: Revisión previa del medio magnético y descarte de acciones irregulares en el medio de backup. Revisión de plan de recuperación de cintas críticas.

Periodicidad: El periodo de backups programados se mantiene inalterable, así como la nomenclatura usada para su control.
No hay un periodo establecido para los restores de usuarios ya que estos se realizan a pedido.

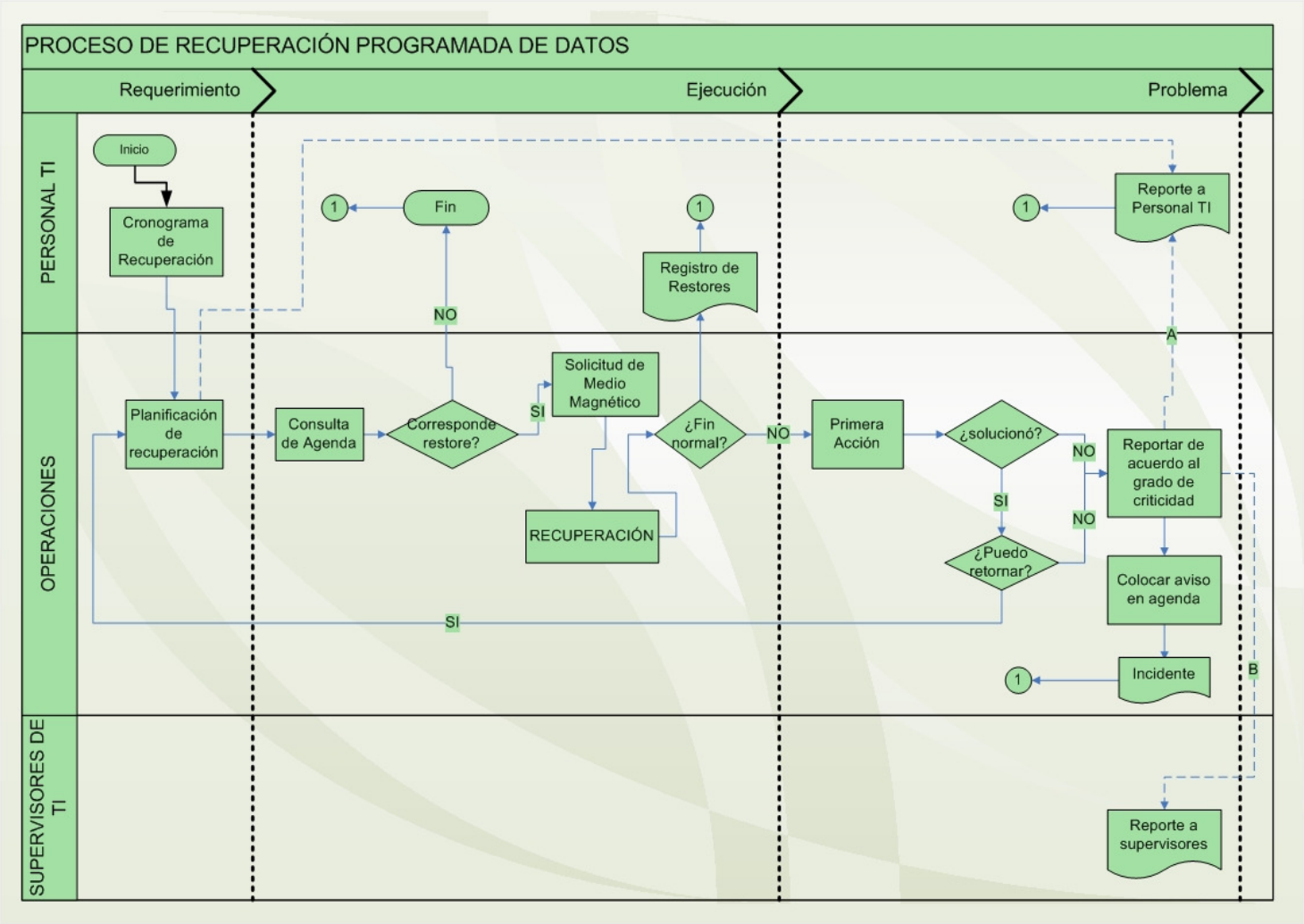
Resguardo:

- Establecer como norma la verificación de datos una vez realizado un resguardo para cualquier tipo de cinta.
- Asegurar el cumplimiento del calendario de backups anual establecido.
- Realización de juego de medios de almacenamiento auxiliar para los sistemas críticos de las locaciones en Lima

Recuperación:

- Realizar revisión de restores de todos los medios existentes. Esto se asegura mediante el cumplimiento del Plan Anual de Verificación y recuperación, por lo que se añadirá un diagrama de procesos y se diferenciará de la solicitud de Restore realizada por los usuarios.
- El procedimiento de recuperación deberá ser probado y comprobado regularmente para verificar y asegurar que son eficaces y que pueden recuperarse en el tiempo que ha sido establecido por los procedimientos operativos

Figura 31. Proceso de Recuperación programada de Datos



Fuente: Elaboración propia

DESECHO DE MEDIOS

Un medio es desechado cuando:

- Se cambia de tecnología de backup (previo copiado de su data a medio con la tecnología actual)
- Presenta errores físicos (cinta rota, sectores dañados)

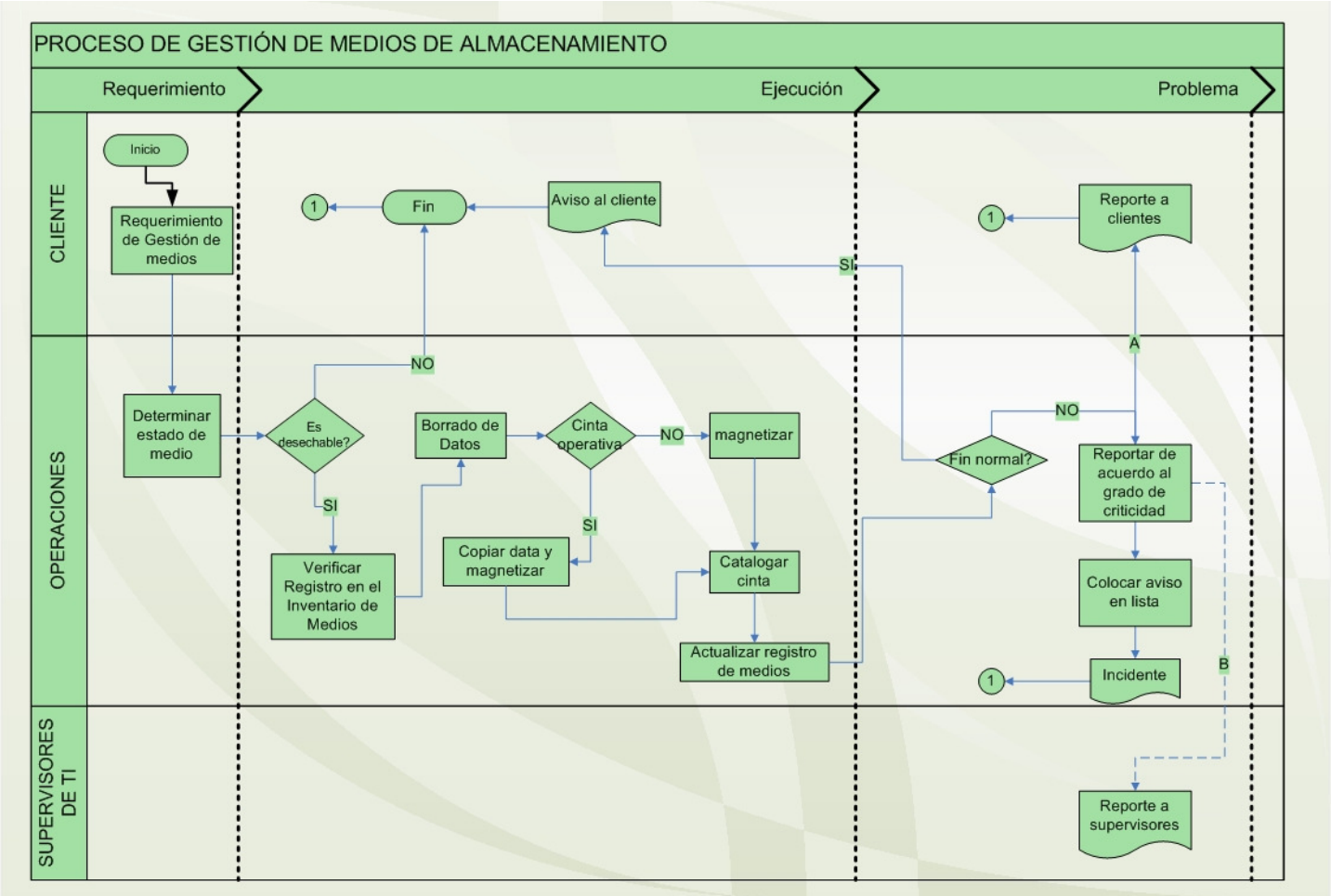
El procedimiento a seguir es el siguiente:

- Personal de operaciones determina el estado del medio.
- Si es medio a desechar, se obtiene el ID físico y lógico del mismo.
- Se verifica su registro en el inventario de medios.
- Se procede al borrado:
    - Si la cinta está operativa se copia la data a otra cinta, y luego se magnetiza
    - Si es imposible leer la cinta, se procede a magnetizarla.
- Una vez borrada la data de las cintas, se catalogan como Reutilizable o Inservible, y se almacena en el ambiente destinado.
- Se actualiza el registro de medios, cambiando el estado de la cinta.

Se debe tomar en cuenta lo siguiente:

- Realizar el etiquetado de aquellos medios que sean considerados no necesarios para su posterior reutilización previa eliminación de los datos allí contenidos.
- Llevar un registro de las cintas que dejarán de ser usadas (desechadas o para su reutilización en caso de requerirlas para pruebas almacenándose en un espacio asignado dentro de las instalaciones.
- Realizar la eliminación de los medios de forma segura cuando son catalogados como inservibles (incinerándolos, triturándolos o vaciando sus datos).

Figura 32. Procedimiento de Desecho de Medios Magnéticos



Fuente: Elaboración propia

6.4.2 Propuesta de indicadores

Los Indicadores están basados en los planteamientos que nos brinda COBIT. La aplicación de cada uno de ellos se realizará de forma mensual.

:

- Frecuencia de las pruebas de los medios de respaldo
  En este indicador se busca garantizar la integridad de los datos una vez culminado el respaldo. Se subdividen de acuerdo al tipo de cinta que se respalda:
  - Frecuencia de prueba de cintas diarias
    Forma de cálculo: (# Días en los que se hizo backup diario / # Pruebas de integridad realizadas a las cintas diarias)
  - Frecuencia de prueba de cintas semanales
    Forma de cálculo: (# Días en los que se hizo backup semanales / # Pruebas de integridad realizadas a las cintas semanales)

- Tiempo promedio del tiempo de restauración de datos.
  Este indicador busca determinar si se cumple con el procedimiento establecido que indica que el tiempo de restauración no debe exceder de 2 minutos por cada GB restaurado.

  Forma de cálculo: $[\sum (M_x / Gb_x)]$ / Total de restores en un mes;
  Donde: M_x = Minutos que se tarda la restauración de la cinta X
  Gb_x = Total de Gigabytes a restaurar de la cinta X

- % de restauraciones de datos exitosas.
  Este indicador nos permite asegurar la completitud, exactitud y accesibilidad de los datos almacenados. La meta a alcanzar es del 100%.
  Forma de Cálculo: (# Restores exitosos / # Total de Restores) * 100%

- # de incidentes en los que se recuperaron datos de medios y equipos ya desechados.
  Este indicador tiene como meta garantizar que los datos marcados como borrados o desechados no puedan recuperarse. Para esto debemos haber definido e implementado los procedimientos que nos permitan prevenir el acceso a datos desde medios una vez que son eliminados o transferidos para otro uso.
  La forma de medir es a través de los logs de resultados una vez realizada la prueba de restauración de la cinta desechada.

- # de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento

Este indicador tiene como meta garantizar que el proceso de respaldo se realice de manera adecuada según el procedimiento establecido.
La forma de medir es a través de los logs de resultados una vez realizado el respaldo de la cinta que indique que se ha alcanzado la capacidad máxima del medio sin haberse completado el respaldo.

- # de incidentes de falta de servicio o de integridad de información causados por incumplimiento de calendario de respaldos.
  Este indicador tiene como meta garantizar que el proceso de respaldo se realice de manera adecuada según el calendario establecido.
  La forma de medir es a través de los logs de resultados una vez ejecutada la tarea de respaldo que indique que no se ha colocado el medio o que éste no es el adecuado, según la programación.

- Número de eventos donde se presente incapacidad para recuperar información crítica para el proceso de negocio.
  Este indicador tiene como meta garantizar la integridad y confiabilidad de la información que ha sido respaldada y que contiene datos sensibles.
  Obtenemos este indicador a través de los logs de restauración que evidencien una falla en algún punto de ejecución de la tarea.

- Satisfacción del usuario con la disponibilidad de la información.
  La meta de este indicador es lograr la total satisfacción del usuario en lo referido a sus solicitudes de restauración de datos.
  Este indicador se obtiene a través de encuestas realizadas a los usuarios de las diversas áreas que han solicitado el servicio indicado a través del Centro de Solicitud de Servicios que maneja la empresa.

6.5 Ejecutar y evaluar modificaciones propuestas

6.5.1 Testeo de indicadores

El testeo de los indicadores propuestos se hará en base a los datos del ultimo año (logs de respaldos y recuperaciones del año 2008) para ubicar el nivel en el q se encuentra la empresa referente al DS11.

Se obtuvieron los siguientes resultados:

Indicador 1: Frecuencia de las pruebas de los medios de respaldo

- Días Backup: Días en el mes en los que según la programación se realizó el respaldo en una cinta diaria / semanal (Ej. 19 días en el Mes 1)
- Días Verificación: La cantidad de días en los que se realizaron las verificaciones a las cintas diarias / semanales en las que se realizó el resguardo.
- Frecuencia: Es la cantidad de veces que se realiza la prueba al backup. La meta es que la frecuencia sea igual a 1, es decir, por cada backup realizado se ejecute la correspondiente verificación.

- Frecuencia de prueba de cintas diarias

Tabla 18. Frecuencia de prueba de cintas diarias.

Mes	1	2	3	4	5	6	7	8	9	10	11	12
Sitio 1												
Dias Backup	19	16	16	18	17	17	19	16	18	18	16	19
Dias Verificacion	14	15	13	16	9	15	12	14	16	15	13	15
Frecuencia	1.36	1.07	1.23	1.13	1.89	1.13	1.58	1.14	1.13	1.20	1.23	1.27
Sitio 2												
Dias Backup	19	16	16	18	17	17	19	16	18	18	16	19
Dias Verificacion	15	13	11	16	7	14	16	15	15	13	14	14
Frecuencia	1.27	1.23	1.45	1.13	2.43	1.21	1.19	1.07	1.20	1.38	1.14	1.36
Sitio 3												
Dias Backup	19	16	16	18	17	17	19	16	18	18	16	19
Dias Verificacion	14	11	15	14	10	13	12	12	14	15	13	17
Frecuencia	1.36	1.45	1.07	1.29	1.70	1.31	1.58	1.33	1.29	1.20	1.23	1.12

Fuente: Elaboración propia

- Frecuencia de prueba de cintas semanales

Tabla 19. Frecuencia de prueba de cintas semanales.

Mes	1	2	3	4	5	6	7	8	9	10	11	12
Sitio 1												
Dias Backup	4	3	3	4	3	3	4	3	4	3	3	4
Dias Verificacion	3	2	2	2	2	2	3	3	2	3	2	3
Frecuencia	1.33	1.50	1.50	2.00	1.50	1.50	1.33	1.00	2.00	1.00	1.50	1.33
Sitio 2												
Dias Backup	4	3	3	4	3	3	4	3	4	3	3	4
Dias Verificacion	3	3	2	2	3	2	3	3	2	2	3	2
Frecuencia	1.33	1.00	1.50	2.00	1.00	1.50	1.33	1.00	2.00	1.50	1.00	2.00
Sitio 3												
Dias Backup	4	3	3	4	3	3	4	3	4	3	3	4
Dias Verificacion	3	3	2	3	2	3	2	2	3	3	2	3
Frecuencia	1.33	1.00	1.50	1.33	1.50	1.00	2.00	1.50	1.33	1.00	1.50	1.33

Fuente: Elaboración propia

Indicador 2: Tiempo promedio del tiempo de restauración de datos.

Tabla 20. Tiempo promedio del tiempo de restauración de datos.

Mes	1	2	3	4	5	6	7	8	9	10	11	12
Sitio 1												
Cant. Restores	4	3	5	2	5	6	5	5	7	4	3	5
∑ Cant. Minutos / Gb (mes)	7	3	11	4	10	13	8	9	12	9	7	10
Promedio Min por Gb	1.75	1.00	2.20	2.00	2.00	2.17	1.60	1.80	1.71	2.25	2.33	2.00
Sitio 2												
Cant. Restores	3	4	8	5	6	4	4	7	5	3	4	6
∑ Cant. Minutos / Gb (mes)	2	9	6	10	14	9	15	13	8	5	7	15
Promedio Min por Gb	0.67	2.25	0.75	2.00	2.33	2.25	3.75	1.86	1.60	1.67	1.75	2.50
Sitio 3												
Cant. Restores	4	2	5	7	3	6	2	4	6	4	4	5
∑ Cant. Minutos / Gb (mes)	10	7	8	3	6	7	6	8	4	9	10	7
Promedio Min por Gb	2.50	3.50	1.60	0.43	2.00	1.17	3.00	2.00	0.67	2.25	2.50	1.40

Fuente: Elaboración propia

Indicador 3: % de restauraciones de datos exitosas.

Tabla 21. Porcentaje de Restauraciones exitosas de Enero a Junio

Mes	1	2	3	4	5	6
Sitio 1						
Cant. Restores exitosos	3	3	4	2	4	6
Cant. Restores	4	3	5	2	5	6
% Restores exitosos	75.0%	100.0%	80.0%	100.0%	80.0%	100.0%
Sitio 2						
Cant. Restores exitosos	2	4	6	4	3	3
Cant. Restores	3	4	8	5	6	4
% Restores exitosos	66.7%	100.0%	75.0%	80.0%	50.0%	75.0%
Sitio 3						
Cant. Restores exitosos	3	1	3	5	3	5
Cant. Restores	4	1	5	7	3	6
% Restores exitosos	75.0%	100.0%	60.0%	71.4%	100.0%	83.3%

Fuente: Elaboración propia

Tabla 22. Porcentaje de Restauraciones exitosas de Julio a Diciembre

Mes	7	8	9	10	11	12
Sitio 1						
Cant. Restores exitosos	3	4	5	3	3	5
Cant. Restores	5	5	7	4	3	5
% Restores exitosos	60.0%	80.0%	71.4%	75.0%	100.0%	100.0%
Sitio 2						
Cant. Restores exitosos	4	5	5	2	4	4
Cant. Restores	4	7	5	3	4	6
% Restores exitosos	100.0%	71.4%	100.0%	66.7%	100.0%	66.7%
Sitio 3						
Cant. Restores exitosos	2	4	4	3	4	5
Cant. Restores	2	4	6	4	4	5
% Restores exitosos	100.0%	100.0%	66.7%	75.0%	100.0%	100.0%

Fuente: Elaboración propia

Indicador 4: # de incidentes en los que se recuperaron datos de medios y equipos ya desechados.

No hay registros durante el 2008 de recuperaciones de datos hechas tomando como origen un medio magnético desechado por lo que el resultado seria cero.

Indicador 5: # de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento

Tabla 23. *:* **# de incidentes por falta de capacidad de almacenamiento.**

Mes	1	2	3	4	5	6	7	8	9	10	11	12
Sitio 1												
# Incidentes	1	0	2	0	0	1	2	1	0	0	0	1
Sitio 2												
# Incidentes	0	0	1	1	0	0	2	1	1	0	1	0
Sitio 3												
# Incidentes	0	0	1	2	0	2	3	1	0	1	0	0

Fuente: Elaboración propia

Indicador 6: # de incidentes de falta de servicio o de integridad de información causados por incumplimiento de calendario de respaldos.

Durante el 2008 sólo se registró un incidente de esta naturaleza durante el mes de Mayo en el Sitio 1, debido al desconocimiento del calendario de backups de nuevo personal contratado para la tarea.

Indicador 7: Número de eventos donde se presente incapacidad para recuperar información crítica para el proceso de negocio.

La información crítica para los procesos de negocio es aquella conformada por los registros de las áreas de Servicios Técnicos y Administración y Finanzas.
Se presentó un incidente durante el mes de Septiembre en donde se perdió parte de un proyecto conteniendo perfiles litológicos recurriéndose al backup full anterior pero éste no contenía toda la información dado que durante el procesos de respaldo estos archivos permanecían en uso y no se había programado backups en caliente.

Indicador 8: Satisfacción del usuario con la disponibilidad de la información.

Este indicador se medirá de acuerdo a la información proporcionada por el área de Atención al Cliente la cual realiza constantes encuestas para determinar la satisfacción del usuario. Se le solicitará un reporte trimestral de las encuestas concernientes a restauraciones de data agrupando las áreas en Administrativa y Técnica.

Tabla 24. Satisfacción del usuario con la disponibilidad de la información.

Trimestre	**1**	**2**	**3**	**4**
Sitio 1				
A. Administrativa	95%	95%	90%	100%
A. Técnica	90%	100%	85%	95%
Sitio 2				
A. Administrativa	75%	90%	95%	100%
A. Técnica	100%	83%	100%	92%
Sitio 3				
A. Administrativa	100%	95%	95%	100%
A. Técnica	80%	95%	100%	95%

Fuente: Elaboración propia

6.5.2 Evaluación de resultados obtenidos en base a indicadores propuestos.

Después de aplicar los cambios planteados, se observó una mayor eficacia en los procesos de resguardo y recuperación de información. Hay que resaltar que se están aplicando los indicadores planteados así como los cambios en los procedimientos en base a los tres primeros meses del año 2009.

Indicador 1: Frecuencia de las pruebas de los medios de respaldo

- Frecuencia de prueba de cintas diarias

Tabla 25. Frecuencia de prueba de cintas diarias - 2009

Mes	1	2	3
Sitio 1			
Días Backup	17	16	16
Días Verificación	16	15	16
Frecuencia	1.06	1.07	1.00
Sitio 2			
Días Backup	17	16	16
Días Verificación	16	16	15
Frecuencia	1.06	1.00	1.07
Sitio 3			
Días Backup	17	16	16
Días Verificación	17	15	16
Frecuencia	1.00	1.07	1.00

Fuente: Elaboración propia

- Frecuencia de prueba de cintas semanales

Tabla 26. Frecuencia de prueba de cintas semanales - 2009

Mes	1	2	3
Sitio 1			
Dias Backup	4	3	3
Dias Verificacion	4	3	2
Frecuencia	1.00	1.00	1.50
Sitio 2			
Dias Backup	4	3	3
Dias Verificacion	3	3	3
Frecuencia	1.33	1.00	1.00
Sitio 3			
Dias Backup	4	3	3
Dias Verificacion	4	3	3
Frecuencia	1.00	1.00	1.00

Fuente: Elaboración propia

Indicador 2: Tiempo promedio del tiempo de restauración de datos.

Tabla 27. Tiempo promedio del tiempo de restauración de datos - 2009

Mes	1	2	3
Sitio 1			
Cant. Restores	6	2	4
∑ Cant. Minutos / Gb (mes)	15	5	8
Promedio Min por Gb	2.50	2.50	2.00
Sitio 2			
Cant. Restores	6	5	7
∑ Cant. Minutos / Gb (mes)	9	10	10
Promedio Min por Gb	1.50	2.00	1.43
Sitio 3			
Cant. Restores	3	5	7
∑ Cant. Minutos / Gb (mes)	7	7	12
Promedio Min por Gb	2.33	1.40	1.71

Fuente: Elaboración propia

Indicador 3: % de restauraciones de datos exitosas.

Tabla 28. Porcentaje de Restauraciones exitosas – 2009

Mes	1	2	3
Sitio 1			
Cant. Restores exitosos	5	2	4
Cant. Restores	6	2	4
% Restores exitosos	83.3%	100.0%	100.0%
Sitio 2			
Cant. Restores exitosos	5	5	7
Cant. Restores	6	5	7
% Restores exitosos	83.3%	100.0%	100.0%
Sitio 3			
Cant. Restores exitosos	3	5	6
Cant. Restores	3	5	7
% Restores exitosos	100.0%	100.0%	85.7%

Fuente: Elaboración propia

Indicador 4: # de incidentes en los que se recuperaron datos de medios y equipos ya desechados.

No hay registros durante los tres primeros meses del 2009 de recuperaciones de datos hechas tomando como origen un medio magnético desechado por lo que el resultado seria cero.

Indicador 5: # de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento

Durante los tres primeros meses del 2009 no se reportaron incidentes de falta o fallas del servicio de resguardo causadas por falta de capacidad de almacenamiento en los medios magnéticos.

Indicador 6: # de incidentes de falta de servicio o de integridad de información causados por incumplimiento de calendario de respaldos.

Durante los tres primeros meses del 2009 no se reportaron incidentes de falta o fallas del servicio de resguardo causadas por incumplimiento de calendario de respaldos.

Indicador 7: Número de eventos donde se presente incapacidad para recuperar información crítica para el proceso de negocio.

Durante los tres primeros meses del 2009 no se reportaron incidentes de falla de recuperación de información crítica. Esto no garantiza que durante los siguientes meses este indicador permanezca en cero.

Indicador 8: Satisfacción del usuario con la disponibilidad de la información.

Tabla 29. Satisfacción del usuario con la disponibilidad de la información - 2009

Trimestre	**1**
Sitio 1	
A. Administrativa	100%
A. Técnica	90%
Sitio 2	
A. Administrativa	95%
A. Técnica	100%
Sitio 3	
A. Administrativa	90%
A. Técnica	100%

Fuente: Elaboración propia

6.6 6ta. Etapa: Publicación de los nuevos procedimientos

6.6.1 Notificación a entes administradores de publicación de documentación

Una vez realizada la propuesta en el procedimiento y la inclusión de otros indicadores se termina de realizar el llenado del FDM (Ficha de Desarrollo de Mejora, Anexo IV), el cual es necesario para regularizar el estudio y la etapa de testeo por el cual pasó el o

los procedimientos, independientemente del resultado de estos. El FDM es un resumen de lo planteado para mejorar uno o más procedimientos o procesos.

Es necesaria presentar esta solicitud para en caso, comprobar la eficacia de los cambios planteados, se pueda proseguir con el trámite para la posterior publicación en el SAD de manera oficial del procedimiento.

En caso contrario, es decir, que no se apruebe los cambios planteados, la ficha FDM pasa a ser parte de un histórico que servirá para próximos planteamientos de mejora.

En los casos estudiados, el FDM es llenado por el analista o CSO responsable, el cual presentará esta ficha al SAD para continuar con la etapa de regularización, publicación y difusión.

La Ficha de Desarrollo de Mejora de los procedimientos aquí analizados se pueden observar en el Anexo IV (Restauración y Resguardo por contingencia)

6.6.2 Puesta en marcha del nuevo procedimiento

Una vez publicados los nuevos procedimientos en el SAD, podrán iniciarse de manera oficial las tareas signadas en el documento así como la obtención de indicadores para la gestión del área. Se dejará evidencia de la prueba de testeo y los resultados obtenidos (indicadores, conclusiones) para evidenciar cualquier posible auditoria posterior.

Al ser un procedimiento con nuevas tareas y especificaciones, las consultas o dudas serán generadas durante los primeros meses lo cual dará pie a una revisión del mismo para corregir pequeños detalles que puedan facilitar la comprensión del personal que es parte responsable en la ejecución de este documento, De esta manera se estará cumpliendo de forma efectiva del ciclo PDCA, en el que la revisión periódica es el factor característico.

Capítulo 7: ANÁLISIS DE RESULTADOS

Una vez realizada la medición en base a los indicadores propuestos tomando como entrada los datos recogidos durante las tareas de resguardo y recuperación ejecutados en el año 2008, se obtuvieron los siguientes resultados:

De acuerdo a nuestro primer indicador, observamos que la frecuencia de prueba de los medios de respaldo se ha incrementado llegando en algunos meses a la meta propuesta, esto es por cada backup ejecutado se realiza la respectiva verificación de datos. Esto asegura la integridad de la información almacenada en los medios. Se consideró solo a las cintas diarias y semanales ya que son las de mayor rotación.

El indicador de tiempo promedio de restauración de datos nos posibilita el pronóstico de disponibilidad de data, logrando asegurar la disponibilidad de la información requerida por los usuarios. El siguiente indicador nos muestra que se ha logrado alcanzar la meta del 100% de restauraciones exitosas en algunos meses. En los meses en los que este porcentaje no ha llegado a la meta ideal se observan como máximo una restauración fallida.

En los cuatro indicadores siguientes, no se reportaron incidencias, por lo consideramos que estos indicadores deben ser medidos tomando periodos mayores de tiempo: semestral o anual.

Los indicadores nos permiten también ayudar en la toma de decisiones a los líderes de TI. Esta toma de decisiones no implica directamente el cambio en el procedimiento sino que interactúa con otro tipo de procesos como son los de calidad.

En cuanto a los cambios en los procedimientos, estos se ejecutaron desde el primes mes del 2009 después de un entrenamiento previo al personal de Operaciones, haciendo énfasis en los modificaciones respecto a las tareas de verificación y recuperación de las cintas críticas

Para esto se planteó tener un cronograma señalando un lapso de tiempo definido para cubrir todo el juego de cintas críticas en los tres sitios y con la frecuencia de un juego de medios mensuales, de esta manera se distribuye la cantidad total de cintas de forma uniforme evitando que se tenga como excusa la premura del tiempo para realizar todas las pruebas en un corto lapso de tiempo. Una vez más, los cambios dieron los resultados esperados cumpliéndose durante el primer trimestre con los restores definidos en el cronograma.

Asimismo, se implementó el procedimiento de desecho de medios magnéticos encontrándose que no existía un inventario de la totalidad de estos. Se definieron los pasos necesarios para la correcta gestión de las cintas, haciendo que la data contenida no pueda ser accesada, evitando así el uso indebido de información de la organización.

Capítulo 8: CONCLUSIONES Y RECOMENDACIONES

Podemos afirmar, que existen gran variedad de estándares de buenas prácticas y normas referentes a la Seguridad de la Información que permiten llevar un mejor control de los procesos que se dan en una empresa, mejorando su eficiencia y eficacia, y que es importante que antes de determinar cual de ellas se va aplicar, la empresa debe conocer sus objetivos, para determinas las acciones necesarias a llevar a cabo que le permitan solucionar sus problemas de seguridad de la información y obtener mejores resultados.

Muchos de las normas y estándares comparten características afines entre ellas. Es por eso que en el caso tomado se utilizó el modelo ISO27002 conjuntamente con COBIT, ya que estas no son excluyentes entre si y sus objetivos de control pueden ser alineados para conseguir una adecuada gestión de la seguridad de la información.

Al obtener los resultados de los indicadores tomando como referencia los datos del año 2008, podemos observar que se lleva a cabo el monitoreo sobre algunas actividades clave de la administración de datos (respaldos, recuperación) dejando de lado el procedimiento de desecho de medios. Además, la responsabilidad de las tareas es asignada de manera informal a personal de TI. A pesar de esto, existe conciencia sobre la necesidad de una adecuada administración de los datos por lo que se plantea la modificación de los procedimientos seguidos hasta entonces.

Tomando en cuenta todas estas características y basándonos en el mapa del nivel de madurez establecido por COBIT, podemos concluir que al momento de iniciar con la metodología planteada este procedimiento se encontraba en el nivel de madurez 2: Repetible pero Intuitivo.

Al implantar los cambios propuestos en los procedimientos y tomando como base los objetivos de control de la norma ISO 27002 para el caso de PetroAmérica se obtuvieron resultados que demuestran que existe una mejora en los procesos, lo cual se ve reflejado en los resultados obtenidos en el primer trimestre del año 2009 y la visible ayuda en la toma de decisiones y oportunidades de mejora. Debemos tener en cuenta que la metodología implantada seguirá un ciclo continuo (PDCA) ya que siempre ocurrirán oportunidades de cambio.

Para implantar esta metodología sobre la base de la norma ISO27002 se debe tener pleno conocimiento de cómo se llevan a cabo los procesos en el área o áreas involucradas, así

como contar con el visto bueno de los jefes de área o en su defecto de la alta gerencia y el apoyo del personal de TI para reducir costos y tiempo.

Ya que los procedimientos de administración de datos se formalizaron dentro de TI (respaldo, recuperación y desecho de medios), se implantaron métricas básicas de desempeño y se llevó a cabo el entrenamiento al personal responsable sobre la administración de información, podemos indicar que se ha llegado al Nivel de madurez 3: Proceso definido

Se recomienda seguir recogiendo datos a través de los indicadores propuestos y continuar con las tareas establecidas en los procedimientos, y así analizar los nuevos resultados generados en un lapso no mayor de 6 meses con el propósito de observarlos para verificar si se ha producido algún cambio favorable que permita que alcancemos el nivel superior inmediato en la escala de madurez de COBIT.

Asimismo, se debe continuar con la evaluación de los demás procedimientos de la empresa relacionados a la Seguridad para determinar la madurez de la totalidad de estos y proceder a la modificación e implementación de indicadores.

REFERENCIAS BIBLIOGRÁFICAS

Alexander Servat, Alberto G., Diseño de un sistema de gestión de seguridad de información: óptica ISO 27001:2005**,** Alfaomega, 2007, Bogotá – Colombia

Alexander Servat, Alberto G., ISO 27000.es, Implantación del ISO 27001: 2005 Sistema de gestión de seguridad de la información, www.**iso**27000.es/download/**Implantacion_del_ISO_27001_2005**.pdf, 03/02/2009

Álvarez Zurita, Flor María, Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud, Escuela Politécnica Nacional, Tesis de Pregrado, 2007, Quito –Ecuador

A.S.S. Borghello Cristian, Seguridad Informática sus implicancias e implementación, Universidad Tecnológica Nacional, Tesis de Licenciatura, 2001, Buenos Aires – Argentina

Atsec, ISMS Implementation Guide**,** Atsec information Security Corporation, www.atsec.com, 25/01/2009

Betarte Gustavo, Corti Maria Eugenia, De la Fuente Reynaldo, Hacia una implementación exitosa de un SGSI, CIBSI, cibsi05.inf.utfsm.cl/presentaciones/sesion11/HaciaUnaImplementacionExitosaDeUnSGSI.pdf, 29/01/2009

Brewer David, Nash Michael, List William, Explotando un sistema de Gestión integrado, ISO 27000.es, www.iso27000.es/download/MSExploitation-SP.pdf, 7/02/2009

Carlson Tom, Lucent Technologies Worldwide Services, Information Security Management: Understanding ISO 17799, www.netbotz.com/library/ISO_17799.pdf, 10/02/2009

Castillo J., ISO 17799: Gestión de seguridad de los sistemas de información, Gestión en el Tercer Milenio, Vol. 5, Nº 10**,** 1728-2969, 2003, 9 – 11

Cisco, Cisco Security index, CISCO, https://www.ciscoredaccionvirtual.com/redaccion/comunicados/comunicado.asp, 03/01/09

Cerini, M., Prá I., Plan de Seguridad Informática, Universidad Católica de Córdoba, http://www.uccor.edu.ar/biblioteca/biblioteca_campus?sec=2&pag=610, 16/02/2009

Chalico Carlos, Ricardo Lira, Analizando las Estrategias del juego 10º encuesta global de seguridad de la información, www.ey.com/mx, 25/01/09

Chapin A., Akridge S., ¿Cómo Puede Medirse la Seguridad?, Information systems control journal , Volume 2, 2005

eEye Digital Security and ECSC Ltd Whitepaper, Information Security Risk Assessments The Special Case of IT Vulnerability Assessments, www.17799.com/papers/BS7799whitepaper.pdf, 10/01/2009

Fernández del Val, Carlos T., Propuesta de introducción de servidores de seguridad en redes y sistemas públicos de comunicaciones, Universidad Politécnica de Madrid, Tesis Doctoral, 1990, Madrid-España

Fernández Domínguez, José Manuel, Grupo Nexus Consultores y Asesores, Parametros fundamentales para la implantación de un sistema de gestión de seguridad e la información según ISO 27001:2005, www.nexusasesores.com, 12/02/2009

Formento H., Manual de Entrenamiento para Equipos de Mejora Continua**, I**nstituto de Industria, Colección Publicación Electrónica N° 3, 2006, Los Polvorines, Bs. As. Argentina

Galanakis A., Risk Assessment Methodology, Information Security Community portal, http://www.17799.com/modules.php, 15/02/09

Grembergen W., De Haes S., COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade1, Information systems control journal, Volume 6, 2005

Hernández Cruz E., Navarrete Pérez E., Sistema de cálculo de indicadores para el mantenimiento, Centro de Estudio de Innovación y Mantenimiento, http://www.mantenimientomundial.com/sites/mmnew/bib/articulos/6calculo.asp, 25/02/2009

Hopkinson Jphn P., The Relationship Between the SSE-CMM and IT Security Guidance Documentation, http://www.sse-cmm.org/docs/sse-guides.pdf, 08/01/09

Information Security Forum (ISF), The Standard of Good Practice for Information Security, https://www.isfsecuritystandard.com/SOGP07/index.htm, 08/01/09

IT Governance Institute, COBIT 4.0, http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf, 08/01/09

ISM3 Consortium, Information Security Management Maturity Model v2.10, http://www.ism3.com/, 08/01/09

ISM3 Consortium, Information Security Glossary, http://www.ism3.com/, 08/01/09

ISO, ISO and International Standards for security, http://www.iso.org, 08/01/09

IT Governance Institute, Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, http://www.isaca.org, 08/01/19

López Neira Agustín, ISO 27000.es, SGPI: Privacidad y beneficio económico en un SGSI, www.iso27000.es/download/SGPI_beneficios_economicos_SGSI.pdf, 01/02/2009

Magdits , Alejandro, Diplomado en Auditoría y Seguridad de Tecnologías de Información COMMON Información, Ernst & Young, www.ey.com, 08/01/09

Medina Iriarte, Johanna, Estándares para la seguridad de Información con tecnologías de información, Universidad de Chile, Tesis de Pregrado, 2006, Santiago-Chile

Microsoft TechNet, Webcast Academia de Seguridad, http://www.microsoft.com/latam/technet/video/alsi.aspx, 08/01/09

Murillo Cano, Sandra Rocio, ASIS: Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la UDLA, Tesis de Magister, 2001, Puebla-México

Narbona Sarria, Manuel, Cómo construir un sistema de gestión de las tecnologías de la información (SGTI), Consejo Superior de Administración Electrónica, www.csi.map.es/csi/tecnimap/tecnimap_2006/01T_PDF/como%20construir%20un%20sistema.pdf, 16/02/2009

Navarro Antonio, Procesos de Software y métricas de proyecto, Universidad Complutense de Madrid, www.fdi.ucm.es/profesor/anavarro/4._Proceso_de_software_y_metricas_de_proyectos.pdf, 24/03/09

NIST (National Institute of standards and Technology), Performance Measurement Guide for Information Security, http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf, 08/01/09

Olsina Luis, Métricas e Indicadores: Dos Conceptos Claves para Medición y Evaluación, Universidad de Chile, www.ciw.cl/recursos/Charla_**Metricas_Indicadores**.pdf, 10/01/2009

Questetra, Inc., KPI, http://en.q-bpm.org/mediawiki/index.php/KPI, 12/02/9

Reijo M. Zavola, Towards a taxonomy for information security metrics, http://portal.acm.org/citation.cfm?id=1314257.1314266, 2007, 28-30

Romero B., Alfonso, Inche M. Jorge, **Quispe A., Carlos**, Sistemas de información gerencial-SIG: una herramienta de decisión estratégica en la industria, Industrial Data, 5(1), 1810-9993, 2002, 66 – 70

SSE-CMM, Systems Security Engineering Capability Maturity Model Model Document, http://www.sse-cmm.org/model/model.asp, 08/01/09

Van Kessel, Paul, Ernst & Young's 2008 Global Information security survey, Ernst & Young, www.ey.com/security, 25/01/09

Venter H.S., Eloff J. H. P. , A taxonomy for information security Technologies, Elsevier Science Ltd, Volumen 22, Número 4, 2003, 299-307

ANEXO I:

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE ISO 27002

DOMINIO	OBJETIVO DE CONTROL	CONTROL
5. POLÍTICA DE SEGURIDAD	5.1 Política de seguridad de la información	5.1.1 Documento de política de seguridad de la información
		5.1.2 Revisión de la política de seguridad de la información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna	6.1.1 Compromiso de la Dirección con la seguridad de la Información
		6.1.2 Coordinación de la seguridad de la información.
		6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
		6.1.4 Proceso de autorización de recursos para el procesado de la información.
		6.1.5 Acuerdos de confidencialidad.
		6.1.6 Contacto con las autoridades.
		6.1.7 Contacto con grupos de especial interés.
		6.1.8 Revisión independiente de la seguridad de la información.
	6.2 Entidades externas (terceros)	6.2.1 Identificación de los riesgos derivados del acceso de terceros.
		6.2.2 Tratamiento de la seguridad en la relación con los clientes.
		6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.	7.1 Responsabilidad sobre los activos.	7.1.1 Inventario de activos.
		7.1.2 Propiedad de los activos.
		7.1.3 Uso aceptable de los activos.
	7.2 Clasificación de la información.	7.2.1 Directrices de clasificación.
		7.2.2 Etiquetado y manipulado de la información.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	8.1 Antes del empleo.	8.1.1 Funciones y responsabilidades.
		8.1.2 Investigación de antecedentes.
		8.1.3 Términos y condiciones de contratación.
	8.2 Durante el empleo.	8.2.1 Responsabilidades de la dirección.
		8.2.2 Formación y capacitación en seguridad de la información.
		8.2.3 Proceso disciplinario.
	8.3 Cese del empleo o cambio de puesto de trabajo.	8.3.1 Responsabilidad del cese o cambio.
		8.3.2 Devolución de activos.
		8.3.3 Retirada de los de derechos de acceso.
9. SEGURIDAD FÍSICA Y AMBIENTAL.	9.1 Áreas seguras.	9.1.1 Perímetro de seguridad física.
		9.1.2 Controles físicos de entrada.
		9.1.3 Seguridad de oficinas, despachos e instalaciones.
		9.1.4 Protección contra las amenazas externas y de origen ambiental.
		9.1.5 Trabajo en áreas seguras.
		9.1.6 Áreas de acceso público y de carga y descarga.

	9.2 Seguridad de los equipos.	9.2.1 Emplazamiento y protección de equipos.
		9.2.2 Instalaciones de suministro.
		9.2.3 Seguridad del cableado.
		9.2.4 Mantenimiento de los equipos.
		9.2.5 Seguridad de los equipos fuera de las instalaciones
		9.2.6 Reutilización o retirada segura de equipos.
		9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	10.1 Responsabilidades y procedimientos de operación.	10.1.1 Documentación de los procedimientos de operación.
		10.1.2 Gestión de cambios.
		10.1.3 Segregación de tareas
		10.1.4 Separación de los recursos de desarrollo, prueba y operación.
	10.2 Gestión de la provisión de servicios por terceros.	10.2.1 Provisión de servicios.
		10.2.2 Supervisión y revisión de los servicios prestados por terceros.
		10.2.3 Gestión de cambios en los servicios prestados por terceros.
	10.3 Planificación y aceptación del sistema.	10.3.1 Gestión de capacidades.
		10.3.2 Aceptación del sistema.
	10.4 Protección contra código malicioso y descargable.	10.4.1 Controles contra el código malicioso.
		10.4.2 Controles contra el código descargado en el cliente.
	10.5 Copias de seguridad	10.5.1 Copias de segundad de la Información.
	10.6 Gestión de la seguridad de las redes	10.6.1 Controles de red.
	10.6 Gestión de la seguridad de las redes	10.6.2 Seguridad de los servicios de red.
	10.7 Gestión de soportes	10.7.1 Gestión de soportes extraíbles
		10.7.2 Eliminación de soportes
		10.7.3 Procedimientos de manipulación de la información
		10.7.4 Seguridad de la documentación del sistema.
	10.8 Intercambio de información.	10.8.1 Políticas y procedimientos de intercambio de información.
		10.8.2 Acuerdos de intercambio
		10.8.3 Soportes físicos en tránsito
		10.8.4 Mensajería electrónica.
		10.8.5 Sistemas de información empresariales.
	10.9 Servicios de comercio electrónico.	10.9.1 Comercio electrónico
		10.9.2 Transacciones en línea.
		10.9.3 Información puesta a disposición pública
	10.10 Supervisión y monitoreo.	10.10.1 Registro de auditorias.
		10.10.2 Supervisión del uso del sistema
		10.10.3 Protección de la información de los registros.
		10.10.4 Registros de administración y operación.
		10.10.5 Registro de fallas
		10.10.6 Sincronización del reloj

11. CONTROL DE ACCESO.	11.1 Requisitos de negocio para el control de acceso.	1 1.1 Política de control de acceso.
	11.2 Gestión del acceso de usuario.	11.2.1 Registro de usuario.
		11.2.2 Gestión de privilegios.
		11.2.3 Gestión de contraseñas de usuario.
		11.2 4 Revisión de los derechos de acceso de usuario.
	11.3 Responsabilidades de usuario.	11.3.1 Uso de contraseña.
		11.3.2 Equipo de usuario desatendido.
		11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
	11.4 Control de acceso a la red.	11.4.1 Política de uso de los servicios en red.
		11.4.2 Autenticación de usuario para conexiones externas.
		11.4.3 Identificación de equipos en las redes.
		11.4.4 Diagnóstico remoto y protección de los puertos de configuración.
		11.4.5 Segregación de las redes.
		11.4.6 Control de la conexión a la red.
		11.4.7 Control de encaminamiento de red.
	11.5 Control de acceso al sistema operativo.	11.5.1 Procedimientos seguros de inicio de sesión.
		11.5.2 Identificación y autenticación de usuario.
		11.5.3 Sistema de gestión de contraseñas.
		11.5.4 Uso de los recursos del sistema.
		11.5.5 Desconexión automática de sesión.
		11.5.6 Limitación del tiempo de conexión.
	11.6 Control de acceso a las aplicaciones y a la información.	11.6.1 Restricción del acceso a la información.
		11.6.2 Aislamiento de sistemas sensibles.
	11.7 Ordenadores portátiles y teletrabajo.	11.7.1 Ordenadores portátiles y comunicaciones móviles.
		11.7.2 Teletrabajo
12. ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	12 1 Requisitos de seguridad de los sistemas de información	12.1 1 Análisis y especificación de los requisitos de seguridad.
	12.2 Tratamiento correcto de las aplicaciones.	12.2.1 Validación de los datos de entrada.
		12.2.2 Control del procesamiento interno.
		122.3 Integridad de los mensajes.
		12.2.4 Validación de los datos de salida.
	12.3 Controles criptográficos.	12.3.1 Política de uso de los controles criptográficos.
		12.3.2 Gestión de claves
	12.4 Seguridad de los archivos de sistema.	12.4.1 Control del software en explotación.
		12.4.2 Protección de los datos de prueba del sistema.
		12.4.3 Control de acceso al código fuente de los programas.
	12.5 Seguridad en los procesos de desarrollo y soporte.	12.5.1 Procedimientos de control de cambios.
		12.5.2 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo.
		12.5.3 Restricciones a los cambios en los paquetes de software.
		12.5.4 Fugas de información.

		12.5.5 Extemalización del desarrollo de software.
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	13.1 Notificación de eventos y puntos débiles de la Seguridad de la información.	13.1.1 Notificación de los eventos de seguridad de la Información.
		13.1.2 Notificación de puntos débiles de la seguridad.
	13.2 Gestión de incidentes de seguridad de la información y mejoras.	13.2.1 Responsabilidades y procedimientos.
		13.2.2 Aprendizaje de los incidentes de segundad de la Información.
		13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
		14.1.2 Continuidad del negocio y evaluación de riesgos.
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
		14.1.4 Marco de referencia para la planificación de la continuidad del negocio.
		14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.	15.1 Cumplimiento de los requisitos legales	15.1.1 Identificación de la legislación aplicable.
		15.1.2 Derechos de propiedad intelectual (DPI).
		15.1.3 Protección de los documentos de la organización.
		15.1.4 Protección de datos y privacidad de la información personal.
		15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información.
		15.1.6 Regulación de los controles criptográficos.
	15.2 Cumplimiento de las políticas y normas de segur y cumplimiento técnico.	15.2.1 Cumplimiento de las políticas y normas de seguridad.
		15.2.2 Comprobación del cumplimiento técnico.
	15.3 Consideraciones de las auditorias de los sistemas de información.	15.3.1 Controles de auditoria de los sistemas de información.
		15.3.2 Protección de las herramientas de auditoria de los sistemas de informo

ANEXO II
PROCESOS DE COBIT

Monitoreo

M1 Monitorear los procesos
M2 Evaluar lo adecuado del control Interno
M3 Obtener aseguramiento independiente
M4 Proveer auditoría independiente

Planeación y Organización

PO1 Definir un Plan Estratégico de TI
PO2 Definir la Arquitectura de Información
PO3 Determinar la dirección tecnológica
PO4 Definir la Organización y Relaciones de TI
PO5 Manejar la Inversión en TI
PO6 Comunicar las directrices gerenciales
PO7 Administrar Recursos Humanos
PO8 Asegurar el cumplir Requerimientos Externos
PO9 Evaluar Riesgos
PO10 Administrar proyectos
PO11 Administrar Calidad

Adquisición e Implementación

AI1 Identificar Soluciones
AI2 Adquisición y Mantener Software de Aplicación
AI3 Adquirir y Mantener Arquitectura de TI
AI4 Desarrollar y Mantener Procedimientos relacionados con TI
AI5 Instalar y Acreditar Sistemas
AI6 Administrar Cambios

Servicios y Soporte

DS1 Definir niveles de servicio
DS2 Administrar Servicios de Terceros
DS3 Administrar Desempeño y Calidad
DS4 Asegurar Servicio Continuo
DS5 Garantizar la Seguridad de Sistemas
DS6 Identificar y Asignar Costos
DS7 Capacitar Usuarios
DS8 Asistir a los Clientes de TI
DS9 Administrar la Configuración
DS10 Administrar Problemas e Incidentes
DS11 Administrar Datos
DS12 Administrar Instalaciones
DS13 Administrar Operaciones

ANEXO III
GLOSARIO DE ACRÓNIMOS Y SISTEMAS

- **Aprobador:** responsable de aprobar un estándar. Es el responsable de las áreas que ejecutan los estándares.
- **CSO:** Chief Security Officer
- **CPD:** Centro de Procesos de Datos
- **Editor:** Cualquier persona, que elabora y edita un estándar. Normalmente es la persona que ejecuta las tareas o actividades a estandarizar.
- **FDM**: Ficha de Desarrollo y Mejora, documento en donde se describen principalmente los cambios propuestos en los procesos, y las mejoras que se obtienen.
- **Gestor:** responsable de promover la elaboración, implantación y control de un estándar. Normalmente es el principal responsable de ejecutar el proceso o actividad al que se refiere el estándar.
- **GP:** Grupo de Práctica,
- **GAP: Brecha,** herramienta de evaluación que permite al Cliente comparar sus procesos actuales contra procesos del mercado relacionados con Seguridad Informática.
- **GRC:** Gerente de Relacionamiento con el Cliente
- **Homologador:** Equipo involucrado en la aceptación operativa de un proceso, normalmente compuesto por todos o los principales afectados.
- I**EC:** International Electrotechnical Commission
- **Proceso:** en el ámbito del documento, para simplificar la redacción) la palabra proceso puede referenciar a un proceso, subproceso o procedimiento de ejecución indistintamente.
- **PNQ:** Premio Nacional de calidad
- **Evaluación ROSI: Return Of Security Investment, Retorno de la inversion de seguridad,** mide la relación entre el retorno que produce una inversión y la inversión propiamente dicha.
- **SAD**: Sistema de Administración de Documentos de la empresa PetroAmerica Este sistema permite agilizar el flujo de elaboración, aprobación, revisión y cancelación de documentos (normativos, procedimientos, manuales y especificaciones) que fundamentan el Sistema de Calidad, ISO 9000 e ISO 14001. SAD también permite la consulta On-Line a más de 37.600 documentos, aproximadamente 10,4 GB de datos, economizando una gran cantidad de papeles.
- **SGC:** Sistema de Gestión de Calidad
- **SOX:** Sarbanes Oxley, Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista
- **TI:** Tecnología de la Información de la empresa.